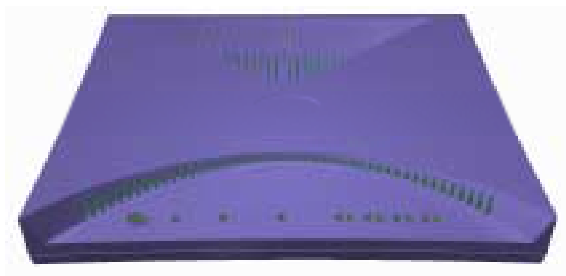


NETOPIA™ 4753 G.SHDSL INTEGRATED ACCESS DEVICE

Administration Guide



netopia®

Copyright

©2001 Netopia, Inc., v.051601

All rights reserved. Printed in the U.S.A.

This manual and any associated artwork, software, and product designs are copyrighted with all rights reserved. Under the copyright laws such materials may not be copied, in whole or part, without the prior written consent of Netopia, Inc. Under the law, copying includes translation to another language or format.

Netopia, Inc.

2470 Mariner Square Loop

Alameda, CA 94501-1010

U.S.A.

Part Number

For additional copies of this electronic manual, order Netopia part number 6161091-PF-01.

Part I: Getting Started

Chapter 1 — Introduction.....	1-1
Overview	1-1
Features and Capabilities	1-1
How to Use This Guide	1-2
Chapter 2 — Setting Up Internet Services	2-1
Definition of Terms.....	2-1
Finding an Internet Service Provider	2-2
Unique requirements.....	2-2
Pricing and support.....	2-2
Endorsements	2-2
Deciding on an ISP Account	2-2
Setting up a Netopia 4753 account.....	2-3
Obtaining an IP address	2-3
Obtaining Information from the ISP.....	2-3
Local LAN IP address information to obtain.....	2-3
Chapter 3 — Making the Physical Connections.....	3-1
Find a Location	3-1
What You Need	3-2
Important Safety instructions	3-3
Identify the Connectors and Attach the Cables	3-4
Netopia 4753 Status Lights.....	3-5
Chapter 4 — Sharing the Connection.....	4-1
Configuring TCP/IP on Windows-based Computers	4-2
Dynamic configuration (recommended)	4-2
Static configuration (optional)	4-3
Configuring TCP/IP on Macintosh Computers	4-5
Dynamic configuration (recommended)	4-5
Static configuration (optional)	4-6

Chapter 5 — Connecting to Your Local Network.....	5-1
Readying Computers on Your Local Network.....	5-2
Connecting to an IP and Telephone Network.....	5-3
Chapter 6 — Console-Based Management	6-1
Connecting through a Telnet Session.....	6-2
Configuring Telnet software	6-2
Connecting a Console Cable to Your Device	6-3
Navigating through the Console Screens.....	6-5
Chapter 7 — Easy Setup	7-1
Easy Setup Console Screens	7-1
Accessing the Easy Setup console screens.....	7-1
Quick Easy Setup Connection Path.....	7-3
DSL Line Configuration	7-5
Voice Easy Setup	7-6
Easy Setup Profile.....	7-7
IP Easy Setup	7-8
Easy Setup Security Configuration	7-9
Chapter 8 — Voice Configuration.....	8-1
Introduction.....	8-1
Explanation of terms	8-1
Configuring the Voice Features	8-2

Part II: Advanced Configuration

Chapter 9 — WAN and System Configuration	9-1
WAN Configuration	9-2
Multiple ATM Permanent Virtual Circuit Support	9-3
Multiple ATM PVC overview	9-3
Multiple ATM PVC configuration	9-4
Changing a circuit	9-5
Adding a circuit.....	9-7
Monitoring multiple virtual circuits.....	9-8

Creating a New Connection Profile.....	9-10
The WAN Default Profile.....	9-13
IP Parameters (Default Profile) screen	9-14
The ATMP/PPTP Default Profile	9-15
System Configuration Screens	9-15
Navigating through the System Configuration screens.....	9-15
System Configuration Features	9-16
Network protocols setup.....	9-17
Filter sets.....	9-17
IP address serving.....	9-17
Date and time (Network Time Protocol).....	9-17
Console configuration.....	9-19
SNMP (Simple Network Management Protocol).....	9-20
Security.....	9-20
Upgrade feature set	9-20
Logging	9-20
Installing the Syslog client	9-21
Chapter 10 — IP Setup	10-1
IP Setup.....	10-2
IP subnets.....	10-4
Static routes	10-6
IP Address Serving	10-10
IP Address Pools.....	10-13
DHCP NetBIOS Options	10-15
More Address Serving Options.....	10-17
Configuring the IP Address Server options	10-18
DHCP Relay Agent.....	10-23
Connection Profiles	10-25
Chapter 11 — Multiple Network Address Translation	11-1
Overview	11-1
Features	11-1

Supported traffic	11-5
MultiNAT Configuration	11-6
Easy Setup Profile configuration	11-6
Server Lists and Dynamic NAT configuration.....	11-6
IP setup	11-7
Modifying map lists	11-13
Moving maps	11-15
Adding Server Lists	11-17
Modifying server lists	11-20
Deleting a server	11-22
Binding Map Lists and Server Lists	11-23
IP profile parameters.....	11-23
IP Parameters (WAN Default Profile)	11-25
NAT Associations	11-27
MultiNAT Configuration Example	11-29
Chapter 12 — Virtual Private Networks (VPNs).....	12-1
Overview	12-1
About PPTP Tunnels	12-3
PPTP configuration	12-4
About IPsec Tunnels.....	12-7
Configuration	12-7
IP Profile Parameters.....	12-10
Advanced IP Profile Options	12-11
Interoperation with other features	12-12
Encryption Support	12-12
ATMP/PPTP Default Answer Profile	12-13
VPN QuickView	12-14
Dial-Up Networking for VPN	12-15
Installing PPTP and Configuring Dial-up	
Networking on a PPTP Client	12-15
About ATMP Tunnels.....	12-19
ATMP configuration	12-19

Allowing VPNs through a Firewall	12-21
PPTP example.....	12-23
ATMP example	12-26
Chapter 13 — Security	13-1
Suggested Security Measures.....	13-1
User Accounts	13-1
Telnet Access	13-3
About Filters and Filter Sets.....	13-4
What's a filter and what's a filter set?	13-4
How filter sets work	13-4
How individual filters work	13-6
Design guidelines	13-10
Working with IP Filters and Filter Sets	13-11
Adding a filter set.....	13-12
Viewing filter sets	13-15
Modifying filter sets.....	13-16
Deleting a filter set	13-16
A sample IP filter set.....	13-16
Firewall Tutorial	13-19
General firewall terms	13-19
Basic IP packet components.....	13-20
Basic protocol types.....	13-20
Firewall design rules	13-21
Filter basics.....	13-23
Example filters.....	13-24
LAN IP Filtersets	13-27
RADIUS Client Support.....	13-30
RADIUS client configuration	13-30
Warning alerts.....	13-32
Chapter 14 — Monitoring Tools	14-1
Quick View Status Overview.....	14-1
General status.....	14-2

Current status	14-3
Status lights.....	14-3
Statistics & Logs	14-4
Event Histories	14-4
WAN Event History	14-5
Device Event History	14-6
Voice Logs.....	14-7
Voice Log	14-7
Voice Accounting Log.....	14-8
IP Routing Table	14-9
Served IP Addresses.....	14-10
General Statistics	14-11
System Information.....	14-13
SNMP	14-13
The SNMP Setup screen.....	14-14
SNMP traps.....	14-15
Chapter 15 — Utilities and Diagnostics	15-1
Ping.....	15-2
Trace Route.....	15-4
Telnet Client	15-5
Disconnect Telnet Console Session.....	15-6
Factory Defaults	15-6
Transferring Configuration and Firmware Files with TFTP..	15-7
Updating firmware.....	15-7
Downloading configuration files	15-8
Uploading configuration files	15-9
Transferring Configuration and Firmware Files with	
XMODEM.....	15-10
Updating firmware.....	15-10
Downloading configuration files	15-11
Uploading configuration files	15-12
Restarting the System	15-12

Part III: Appendixes

Appendix A — Troubleshooting.....	A-1
Configuration Problems	A-1
Console connection problems	A-2
Network problems.....	A-2
How to Reset the Netopia 4753 to Factory Defaults	A-3
Power Outages	A-3
Technical Support	A-4
How to reach us	A-4
Appendix B — Understanding IP Addressing	B-1
What is IP?.....	B-1
About IP Addressing	B-1
Subnets and subnet masks	B-2
Example: Using subnets on a Class C IP internet ...	B-3
Example: Working with a Class C subnet.....	B-5
Distributing IP Addresses	B-5
Technical note on subnet masking	B-6
Configuration	B-7
Manually distributing IP addresses	B-8
Using address serving.....	B-8
Tips and rules for distributing IP addresses	B-9
Nested IP Subnets	B-11
Broadcasts.....	B-13
Packet header types	B-13
Appendix C — Binary Conversion Table.....	C-1
Appendix D — Further Reading	D-1
Appendix E — Technical Specifications and Safety Information...	E-1
Description.....	E-1
Power requirements	E-1
Environment	E-1
Software and protocols	E-1

Agency Approvals.....	E-2
Regulatory notices	E-2
Important Safety instructions	E-4
Netopia 4753 Specifications	E-5
Physical interface	E-5
Data features	E-5
Hardware specifications	E-7
Voice features	E-7
Glossary.....	1
Index	1
Limited Warranty and Limitation of Remedies	1

Part I: Getting Started

Chapter 1

Introduction

Overview

The Netopia 4753 Voice/Data Integrated Access Devices (IADs) make it possible for small businesses to take advantage of the advanced communications technologies previously limited to larger organizations. By integrating multiple voice connections and high-speed Internet access on one DSL line, businesses can squeeze the most out of their communications budget.

The Netopia 4753 G.SHDSL Integrated Access Device combines a complete telephone system with a business-class data router to deliver a customized package of business communications services over DSL. The Netopia 4753 supports the broad array of phone features offered through your service provider and uses your existing analog telephone equipment. The Netopia 4753 includes Netopia's sophisticated data routing engine optimized for small and medium size business needs. These business-class features include IP routing, firewall, NAT, MultiNAT, DHCP and both PPTP and IPsec VPN functionality.

This section covers the following topics:

- [“Features and Capabilities” on page 1-1](#)
- [“How to Use This Guide” on page 1-2](#)

Features and Capabilities

Office telephone systems are commonly one of two types, PBX (Private Branch Exchange) or Centrex (Central Office Exchange). Technically, Centrex is a subset of PBX.

PBX users share a certain number of outside lines for making telephone calls external to the PBX. Most medium-sized and larger companies use a PBX because it's much less expensive than connecting an external telephone line to every telephone in the organization. In addition, it's easier to call someone within a PBX because the number you need to dial is typically just 3 or 4 digits.

Centrex is a newer variation on the PBX. It is a PBX with all switching occurring at a local telephone office instead of at the company's premises. Typically, the telephone company owns and manages all the communications equipment necessary to implement the PBX and then sells various services to the company.

Small- to medium-sized businesses need two kinds of services: Internet presence and voice telephony. But they don't need the additional burden of maintaining switching equipment or administering IP and voice services for their offices. An Integrated Access Device (IAD) that offers high-speed Symmetric (same speed upload and download) DSL for IP connectivity and a PBX that somebody else (the phone company) administers is the simple solution.

At the phone company's central office, where all the big switch gear is, there are two kinds of switches for the two kinds of services, voice and data. The voice switch is called a Voice Gateway and the data switch is called a Digital Subscriber Line Access Multiplexer (DSLAM) or access concentrator. Both the voice and data signals are concentrated at the DSLAM and forwarded either to a data router or to the Voice Gateway. Both kinds of switches are manufactured by a variety of companies. The IAD must be capable of communicating with a wide array of possible combinations of Voice Gateways and DSLAMs.

1-2 Administration Guide

An IAD combines the voice telephony features of a telephone PBX system with the data routing features of an IP data router. The device uses a single outside line connection to carry all voice and data transmissions. If the device uses a DSL interface, it can carry all of these services over a single existing copper telephone line by using the different frequency ranges available on the copper wire for voice and data traffic.

The Netopia 4753 G.SHDSL Integrated Access Device is that device: a Centrex-based PBX system combined with an SHDSL internet router.

The Netopia 4753 G.SHDSL Integrated Access Device provides the following features:

Support for ordinary analog phone equipment. Works with the same FXS analog phone sets and key systems that small businesses use today. No expensive handsets to order, no new interface to learn.

Centrex support. Advanced telephone features enabled by your service provider's telephone switch such as call forwarding or conferencing operate exactly as they did before.

Netopia data routing engine. Provides the same advanced, business-class data routing features used by leading DSL service providers around the world. Includes advanced data functionality such as firewall, VPN client and server (including PPTP and IPSec), DHCP automated address assignment, and Network Address Translation (NAT and MultiNAT).

Physical features include:

- G.SHDSL WAN Interface interoperable with major ATM- and Frame Relay-based DSL equipment.
- A 10/100 Ethernet LAN Port.
- Eight analog telephone ports (local extensions).
- One DB-9 serial console port.
- Front panel status lights.
- Setup and configuration management via console menu.

How to Use This Guide

This guide is designed to be your source for information about your Netopia 4753 G.SHDSL Integrated Access Device. It is intended to be viewed on-line, using the powerful features of the Adobe Acrobat Reader. The information display has been deliberately designed to present the maximum information in the minimum space on your screen. You can keep this document open while you perform any of the procedures described, and find useful information about the procedure you are performing.

If you prefer to work from hard copy rather than on-line documentation, you can also print out all of the manual, or individual sections. The pages are formatted to print on 8 1/2 by 11 inch paper. We recommend that you print on three-hole punched paper, so you can put the pages in a binder for future reference. For your convenience, a printed copy can be purchased from Netopia. Order part number TEP708/Doc.

This guide is organized into chapters describing the Netopia 4753's advanced features. You may want to read each chapter's introductory section to familiarize yourself with the various features available.

Use the guide's table of contents and index to locate informational topics.

Chapter 2

Setting Up Internet Services

This chapter describes how to obtain and set up Internet services.

This section covers the following topics:

- “Definition of Terms” on page 2-1
- “Finding an Internet Service Provider” on page 2-2
- “Deciding on an ISP Account” on page 2-2
- “Obtaining Information from the ISP” on page 2-3

Note: Some companies act as their own ISP. For example, some organizations have branch offices that can use the Netopia 4753 to access the Internet via the main office in a point-to-point scenario. If you install the Netopia 4753 in this type of environment, refer to the following sections for specific information you must receive from the network administrator to configure the Netopia 4753 properly.

Definition of Terms

G.SHDSL. A rate-adaptive digital communication medium that operates over existing analog telephone lines provided by the telephone company. G.SHDSL negotiates the highest achievable data rate given the loop conditions and will allow you to connect to the Internet at a minimum of 128Kbps bi-directional, up to 2.320 Mbps. Your LAN will constantly be connected and you will not have to dial into the Internet. G.SHDSL uses more of the bandwidth on copper phone lines than what is currently used for plain old telephone service (POTS). By using frequencies between 26 kHz and 1MHz, G.SHDSL can encode more data to achieve higher data rates than would otherwise be possible in the restricted frequency range of a POTS network (up to 4 kHz). In order to use the frequencies above the voice audio spectrum, DSL equipment must be installed on both ends.

Internet Protocol (IP) address. A network address that uniquely identifies a device on an IP network. This type of address consists of 4 bytes, represented as decimal values, separated by periods, e.g., 192.168.2.143. All IP addresses of the form 192.168.1.xxx are private IP addresses.

Media Access Control (MAC) address. This 48 bit address is assigned by the device manufacturer for its Ethernet connection. All Netopia 4753 units have MAC addresses of the form 00-C5-9X-XX-XX-XX. Each byte is represented as a conventional two digit hexadecimal number.

Point-to-Point Protocol (PPP). A serial protocol defined in RFC 1661 that is used to provide point-to-point connectivity over serial links.

Password Authentication Protocol (PAP). A form of PPP authentication that requires an exchange of user names and clear-text passwords between two devices. PAP passwords are sent unencrypted.

Challenge Handshake Authentication Protocol (CHAP). A form of PPP authentication that requires an exchange of user names and secrets (encrypted passwords) between two devices. This security feature is supported on lines using PPP encapsulation. CHAP passwords are called secrets because they are sent encrypted.

Finding an Internet Service Provider

The Netopia 4753 G.SHDSL Integrated Access Device provides its high speed symmetric (two-way) digital connection to the Internet through a Competitive Local Exchange Carrier (CLEC) – a type of mini phone company. The CLEC uses a compatible type of switching equipment known as a Digital Subscriber Line Access Multiplexer (DSLAM). The DSLAM that you connect to with your Netopia Router must be capable of handling these symmetric connections. The Netopia 4753 is certified for use with DSLAMs manufactured by Nokia , Lucent, Paradyne, Nortel networks, and Copper Mountain.

If you have purchased your Netopia Router through a Netopia ISP partner, you can be sure that an account that supports G.SHDSL connections will be available.

If your area has more than one ISP, the following considerations will help you decide which ISP is best suited for your requirements.

In determining which Internet service provider (ISP) to establish your account with, make sure that your ISP supports connections via a CLEC that also supports voice services.

Use an ISP that provides Internet access through a G.SHDSL Digital Subscriber Line and that supports the Netopia 4753 G.SHDSL Integrated Access Device. If you would like to use an ISP that you already have a relationship with but that is not familiar with the Netopia 4753, call us at 1-800-NETOPIA. Our representative can call your ISP and introduce them to the product. If necessary, we will provide them with the technical background they need to support the product.

Unique requirements

Make sure the ISP can meet any unique requirements you may have, such as:

- Dynamic or static IP addressing
- Class C IP address
- Custom domain name
- Multiple e-mail addresses
- Web site hosting

Pricing and support

Compare pricing, service, and technical support service among various ISPs.

Endorsements

Consider recommendations from colleagues and reviews in publications. Netopia lists Netopia Certified ISPs on our Web site at **<http://www.netopia.com>**.

Deciding on an ISP Account

Your ISP may offer various Internet access account plans. Typically, these plans vary by usage charges and the number of host IP addresses supplied. Evaluate your networking needs and discuss them with your ISP before deciding on a plan for your network.

Setting up a Netopia 4753 account

Check whether your ISP has the Netopia 4753 on its list of supported products that have been tested with a particular configuration. If the ISP does not have the Netopia 4753 on such a list, describe the Netopia 4753 in as much detail as needed, so your ISP account can be optimized. As appropriate, refer your ISP to Netopia's Web site www.netopia.com for more information.

Obtaining an IP address

Typically, each network computer that requires Internet access requires its own unique IP address. If some or all network computers require simultaneous Internet access, obtain a block of IP host addresses large enough for each computer to have its own address, plus one for the Netopia 4753.

Consider expected growth in your network when deciding on the number of addresses to obtain. Alternatively, you can use the Network Address Translation feature of SmartIP.

SmartIP

The Netopia 4753 G.SHDSL Integrated Access Device supports Multiple Network Address Translation (MultiNAT).

Network Address Translation provides Internet access to the network connected to the Netopia 4753 using only a single IP address. These routers translate between the internal or local area network (LAN) addresses and a single external IP address, and route accordingly.

For more information on Network Address Translation, see [Chapter 11, "Multiple Network Address Translation."](#)

Obtaining Information from the ISP

After your account is set up, the ISP should send you the IP parameter information that will help you configure the Netopia 4753.

Local LAN IP address information to obtain

Your ISP will need to provide you with the following information:

- The default gateway IP address (same as remote IP address in most cases)
- Local WAN IP address and subnet mask
- Primary and secondary domain name server (DNS) IP addresses
- Domain name (usually the same as the ISP's domain name unless you have registered for your own individual domain name)

Note: The default gateway, WAN address and mask, DNS, and domain name are all obtainable via WAN DHCP, if your ISP supports it.

With Network Address Translation

If you are using MultiNAT, you should obtain the following:

- If you are connecting to a remote site using Network Address Translation on your router, your provider will

2-4 Administration Guide

not define the IP address information on your local LAN. You can define this information based on an IP configuration that may already be in place for the existing network. Alternatively, you can use the default IP address range used by the router.

Without Network Address Translation

If you are not using Network Address Translation, you will need to obtain all of the local LAN IP address information from your ISP.

If you are not using SmartIP (NAT), you should obtain:

- The number of Ethernet IP host addresses available with your account and the first usable IP host address in the address block
- The Ethernet IP address for your Netopia 4753
- The Ethernet IP subnet mask address for your Netopia 4753

Chapter 3

Making the Physical Connections

This section tells you how to make the physical connections to your Netopia 4753 G.SHDSL Integrated Access Device. This section covers the following topics:

- “Find a Location” on page 3-1
- “What You Need” on page 3-2
- “Important Safety instructions” on page 3-3
- “Identify the Connectors and Attach the Cables” on page 3-4
- “Netopia 4753 Status Lights” on page 3-5

Find a Location

Note: Before connecting your Netopia 4753, be sure to read the important safety information contained in Appendix E, “Technical Specifications and Safety Information.”

When choosing a location for the Netopia Router, consider:

- Available space and ease of installation
- Physical layout of the building and how to best use the physical space available for connecting your Netopia Router to the LAN
- Available wiring and jacks
- Distance from the point of installation to the next device (length of cable or wall wiring)
- Ease of access to the front of the unit for configuration and monitoring
- Ease of access to the back of the unit for checking and changing cables
- Cable length and network size limitations when expanding networks

For small networks, install the Netopia 4753 near one of the LANs. For large networks, you can install the Netopia 4753 in a wiring closet or a central network administration site.

What You Need

Locate all items that you need for the installation.

Included in your package are:

- The Netopia 4753 G.SHDSL Integrated Access Device
- A power adapter and cord with a mini-DIN8 connector
- One 6 ft. RJ45 10/100 Ethernet cable
- One 6 ft. RJ45 DSL WAN (or Line) cable
- A DB-9 to DB-9 console cable
- Printed Installation guide
- The Netopia CD containing Adobe Acrobat Reader for Windows and Macintosh, ZTerm terminal emulator software for Classic MacOS and MacOSX and NCSA Telnet for Macintosh, and documentation

You will need:

- A Windows 95 or 98-based PC or a Macintosh computer with Ethernet connectivity for configuring the Netopia 4753. This may be built-in Ethernet or an add-on card, with TCP/IP installed and configured. See [“Sharing the Connection” on page 4-1](#).
- A DSL wall outlet wired for a connection to a Local Exchange Carrier (LEC) who supports G.SHDSL Digital Subscriber Line connections.

Important Safety instructions

CAUTION: Depending on the power supply provided with the product, either the direct plug-in power supply blades, power supply cord plug or the appliance coupler serves as the main power disconnect. It is important that the direct plug-in power supply, socket-outlet or appliance coupler be located so it is readily accessible.

CAUTION (North America Only): For use only with a CSA Certified or UL Listed Limited Power Source or Class 2 power supply, rated 12Vdc, 1.5A.

CAUTION (Europe Only): For use only with a GS approved Limited Power Source, rated 12Vdc, 1.5A.

TELECOMMUNICATION INSTALLATION CAUTIONS

When using your telephone equipment, basic safety precautions should always be followed to reduce the risk of fire, electric shock and injury to persons, including the following:

1. Do not use this product near water, for example, near a bathtub, wash bowl, kitchen sink or laundry tub, in a wet basement or near a swimming pool.
2. Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electrical shock from lightning.
3. Do not use the telephone to report a gas leak in the vicinity of the leak.

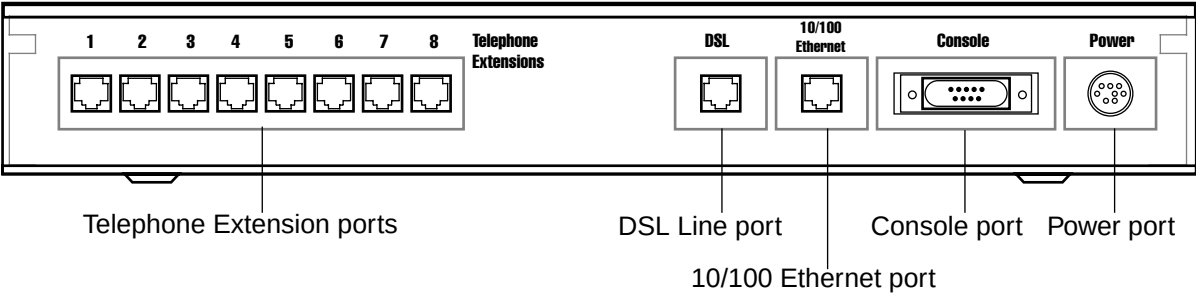
SAVE THESE INSTRUCTIONS

Identify the Connectors and Attach the Cables

Identify the connectors on the back panel and attach the necessary Netopia cables.

The figure below displays the back of the Netopia 4753 G.SHDSL Integrated Access Device.

Netopia 4753 back panel



The following table describes all the Netopia 4753 G.SHDSL Integrated Access Device back panel ports.

Port	Description
Telephone extension ports	Eight RJ-11 telephone jacks for connecting your phone extensions.
DSL port	An RJ-45 10Base-T-style jack labeled DSL for your DSL connection.
Ethernet port	An RJ-45 10/100Base-T Ethernet jack. You will use this to configure the Netopia 4753. For a new installation, use the Ethernet connection. Alternatively, you can use the console connection to run console-based management using a direct serial connection. You can either connect your computer directly the Ethernet port using a crossover cable, or connect both your computer and the Netopia 4753 to an existing Ethernet hub on your LAN.
Console port	A DB-9 console port for a direct serial connection to the console screens. You can use this if you are an experienced user. See “Connecting a Console Cable to Your Device” on page 6-3 .
Power port	A mini-DIN8 power adapter cable connection.

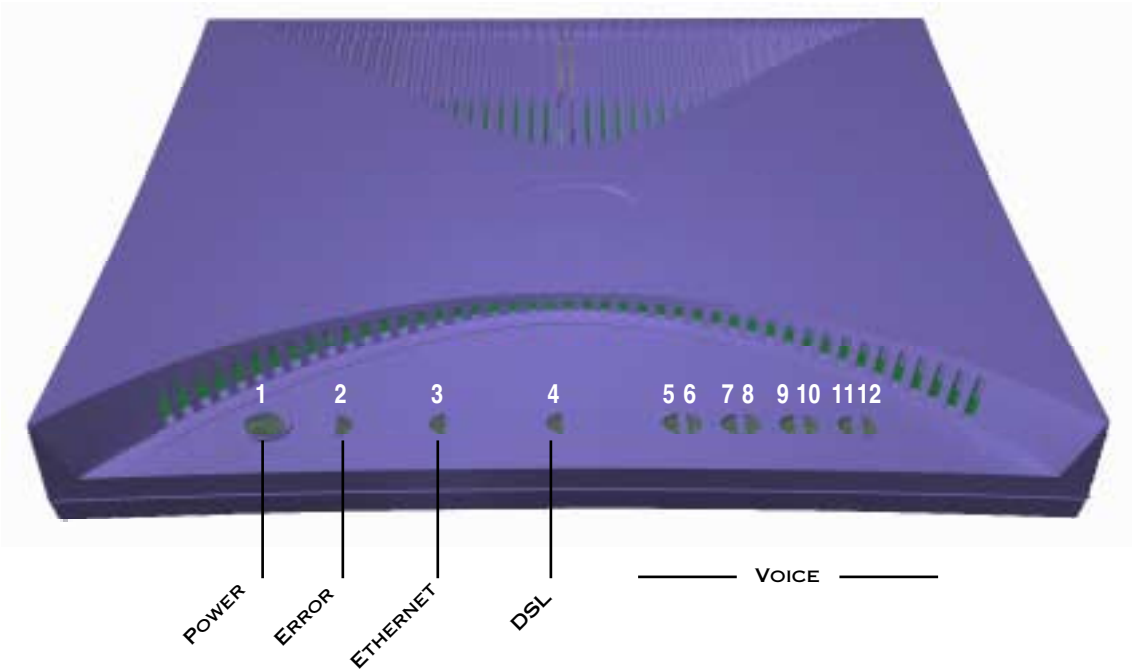
1. Connect the mini-DIN8 connector from the power adapter to the power port, and plug the other end into an electrical outlet.
2. Connect one end of the RJ-45 cable to the DSL port, and the other end to your DSL wall outlet.
3. Connect the Ethernet cable to the Ethernet port on the unit and the other end to your Ethernet hub.

You should now have: the power adapter plugged in; the Ethernet cable connected between the router and your Ethernet hub; and the DSL cable connected between the router and the DSL wall outlet.

Netopia 4753 Status Lights

The figure below represents the Netopia 4753 status light (LED) panel.

Netopia 4753 LED front panel



The following table summarizes the meaning of the various LED states and colors:

When this happens...	the LEDs...
The power is off (button is not pressed in)	1 is dark .
The power is on (button pressed in)	1 is green .
No errors are detected on any interface	2 is dark .
Errors are detected on any interface	2 is red .
The Ethernet interface is operational	3 is green .
The Ethernet interface is disabled	3 is dark .
The DSL WAN interface is inactive	4 is dark .
The DSL WAN interface is training	4 flashes green . Initially the LED is dark, then flashes green while attempting to establish connection to the DSLAM. While exchanging connection information with the DSLAM, the LED flashes slightly faster.
The DSL WAN interface is trained	4 is solid green .
A phone is off-hook	5 through 12 are green for the corresponding extension.
A phone is on-hook	5 through 12 are dark for the corresponding extension.

Chapter 4

Sharing the Connection

Once you have set up your physical local area network, you will need to configure the TCP/IP stack on each client workstation connected to your Netopia 4753. This chapter describes how to configure TCP/IP for both Windows-based and Macintosh computers.

This chapter explains the following topics:

- “Configuring TCP/IP on Windows-based Computers” on page 4-2
- “Configuring TCP/IP on Macintosh Computers” on page 4-5

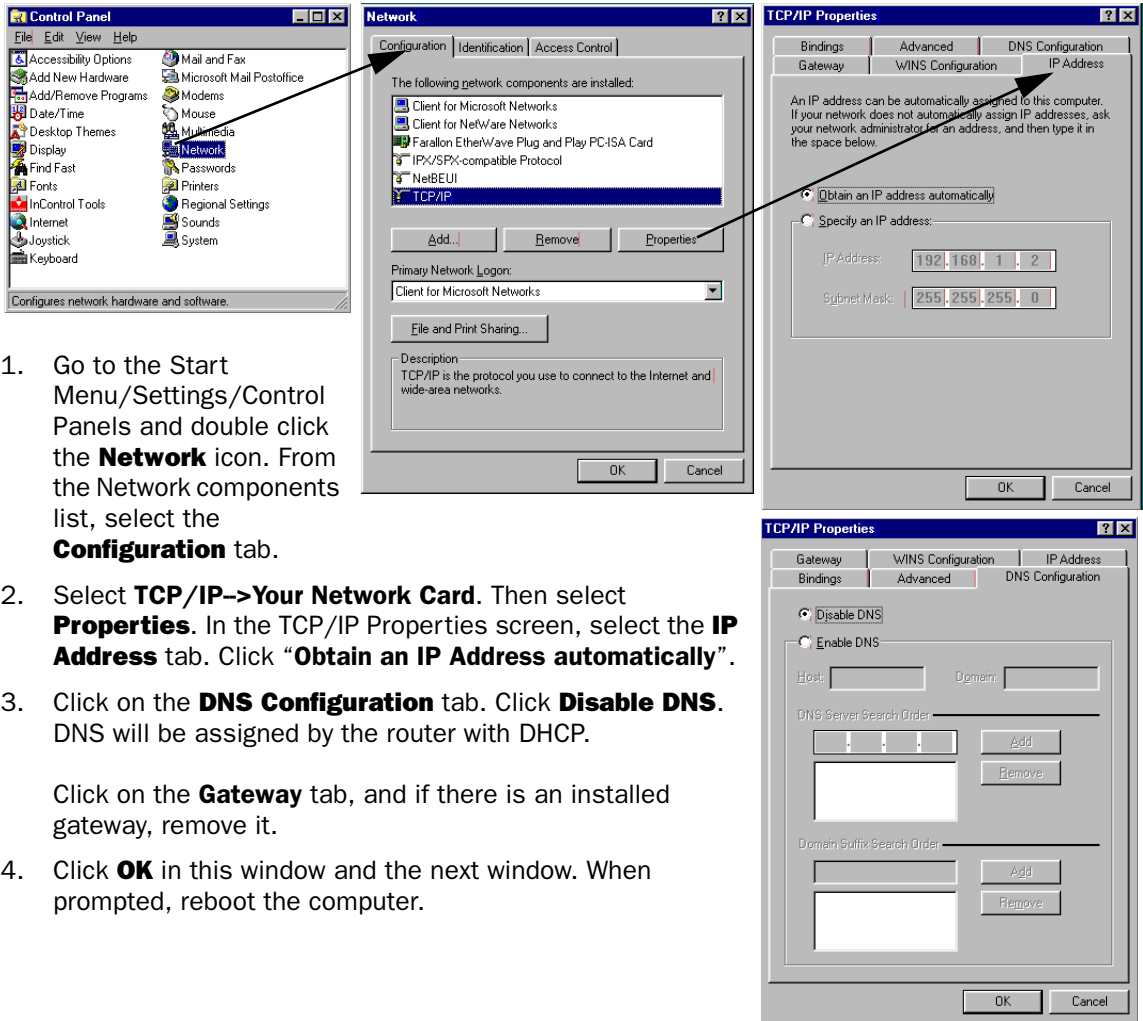
Configuring TCP/IP on Windows-based Computers

Configuring TCP/IP on a Windows computer requires the following:

- An Ethernet card (also known as a network adapter)
- The TCP/IP protocol must be “bound” to the adapter or card

Dynamic configuration (recommended)

To configure your PC for dynamic addressing do the following:



1. Go to the Start Menu/Settings/Control Panels and double click the **Network** icon. From the Network components list, select the **Configuration** tab.
2. Select **TCP/IP→Your Network Card**. Then select **Properties**. In the TCP/IP Properties screen, select the **IP Address** tab. Click “**Obtain an IP Address automatically**”.
3. Click on the **DNS Configuration** tab. Click **Disable DNS**. DNS will be assigned by the router with DHCP.

Click on the **Gateway** tab, and if there is an installed gateway, remove it.

4. Click **OK** in this window and the next window. When prompted, reboot the computer.

Note: You can also use these instructions to configure other computers on your network to accept IP addresses served by the Netopia 4753.

Static configuration (optional)

If you are manually configuring for a fixed or static IP address, perform the following:

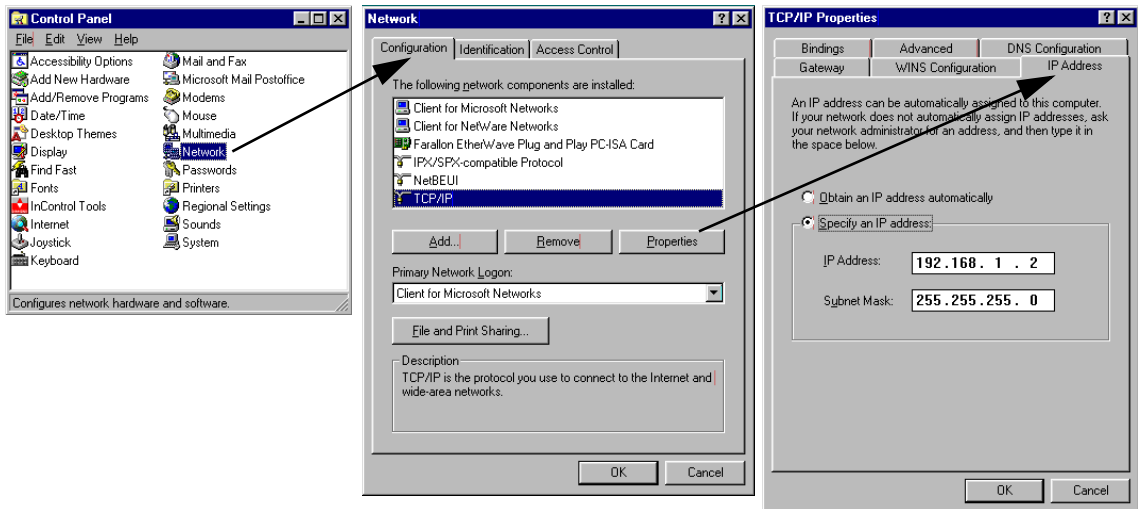
1. Go to Start Menu/Settings/Control Panels and double click the **Network** icon. From the Network components list, select the **Configuration** tab.
2. Select **TCP/IP→Your Network Card**. Then select **Properties**. In the TCP/IP Properties screen, select the **IP Address** tab. Click "**Specify an IP Address.**"

Enter the following:

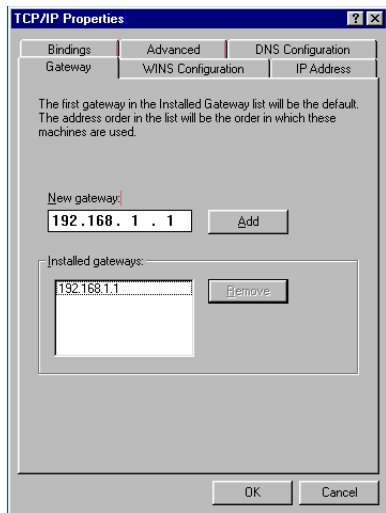
IP Address: 192.168.1.2

Subnet Mask: 255.255.255.0

This address is an example of one that can be used to configure the router. Your ISP or network administrator may ask you to use a different IP address and subnet mask.



3. Click on the **Gateway** tab (shown below). Under “New gateway,” enter **192.168.1.1**. Click **Add**. This is the Netopia 4753’s pre-assigned IP address.



Click on the **DNS Configuration** tab. Click **Enable DNS**. Enter the following information:

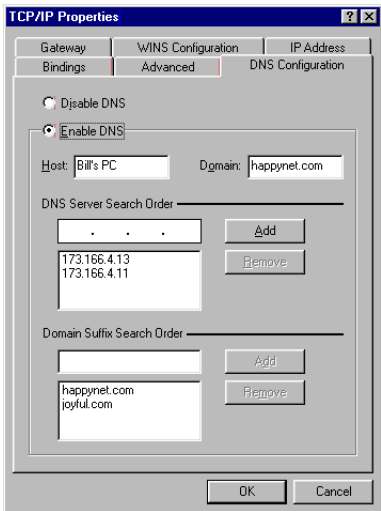
Host: Type the name you want to give to this computer.

Domain: Type your domain name. If you don't have a domain name, type your ISP's domain name; for example, netopia.com.

DNS Server Search Order: Type the primary DNS IP address given to you by your ISP. Click

Add. Repeat this process for the secondary DNS.

Domain Suffix Search Order: Enter the same domain name you entered above.



4. Click **OK** in this window and the next window. When prompted, reboot the computer.

Note: You can also use these instructions to configure other computers on your network with manual or static IP addresses. Be sure each computer on your network has its own IP address.

Configuring TCP/IP on Macintosh Computers

The following is a quick guide to configuring TCP/IP for MacOS computers. Configuring TCP/IP in a Macintosh computer requires the following:

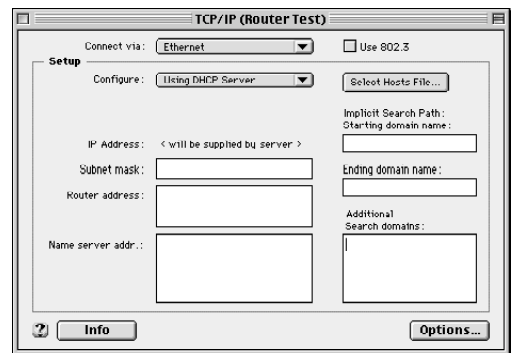
- You must have either Open Transport or Classic Networking (MacTCP) installed.

Note: If you want to use the Dynamic Host Configuration Protocol (DHCP) server built into your Netopia 4753 to assign IP addresses to your Macintoshes, you must be running Open Transport, standard in MacOS 8 and optional in earlier system versions. You can have your Netopia 4753 dynamically assign IP addresses using MacTCP; however, to do so requires that the optional AppleTalk kit be installed which can only be done after the router is configured.
- You must have built-in Ethernet or a third-party Ethernet card and its associated drivers installed in your Macintosh.

Dynamic configuration (recommended)

The Dynamic Host Configuration Protocol (DHCP), which enables dynamic addressing, is enabled by default in the router. To configure your Macintosh computer for dynamic addressing do the following:

1. Go to the Apple menu. Select **Control Panels** and then **TCP/IP**.
2. With the TCP/IP window open, go to the Edit menu and select **User Mode**. Choose **Basic** and click **OK**.
3. In the TCP/IP window, select “**Connect via: Ethernet**” and “**Configure: Using DHCP Server.**”



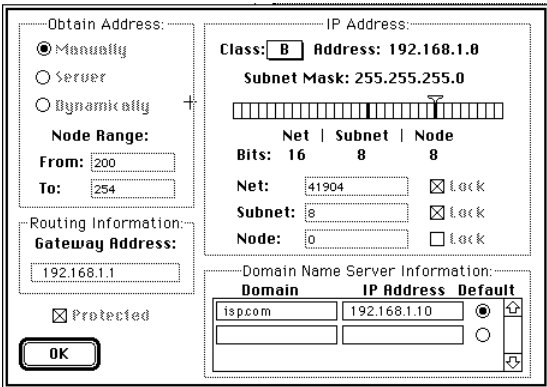
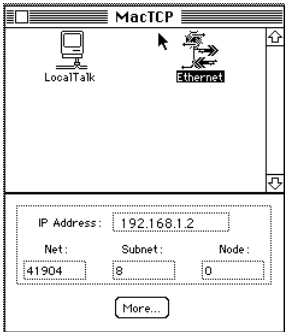
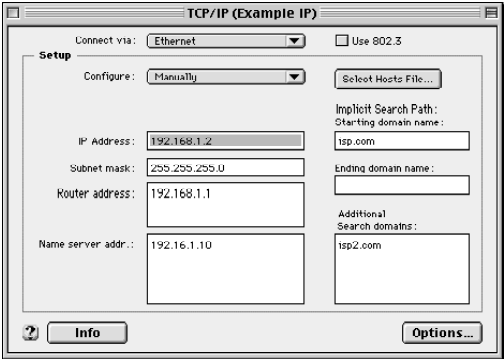
Note: You can also use these instructions to configure other computers on your network to accept IP addresses served by the Netopia 4753.

Static configuration (optional)

If you are manually configuring for a fixed or static IP address, perform the following:

- 1. Go to the Apple menu. Select **Control Panels** and then **TCP/IP** or **MacTCP**.
- 2. With the TCP/IP window open, go to the Edit menu and select **User Mode**. Choose **Advanced** and click **OK**.

Or, in the MacTCP window, select **Ethernet** and click the **More** button.



- 3. In the TCP/IP window or in the MacTCP/More window, select or type information into the fields as shown in the following table.

Option:	Select/Type:
Connect via:	Ethernet
Configure:	Manually
IP Address:	192.168.1.2
Subnet mask:	255.255.255.0, or for 12-user models 255.255.255.240
Router or Gateway address:	192.168.1.1
Name server address:	Enter the primary and secondary name server addresses given to you by your ISP
Implicit Search Path: Starting domain name:	Enter your domain name; if you do not have a domain name, enter the domain name of your ISP

- 4. Close the TCP/IP or MacTCP control panel and save the settings.
- 5. If you are using MacTCP, you must restart the computer. If you are using Open Transport, you do not need to restart.

Note: You can also use these instructions to configure other computers on your network with manual or static IP addresses. Be sure each computer on your network has its own IP address.

More information about configuring your Macintosh computer for TCP/IP connectivity through a Netopia 4753 can be found in Technote NIR_026, "Open Transport and Netopia Routers," located on the Netopia Web site.

Chapter 5

Connecting to Your Local Network

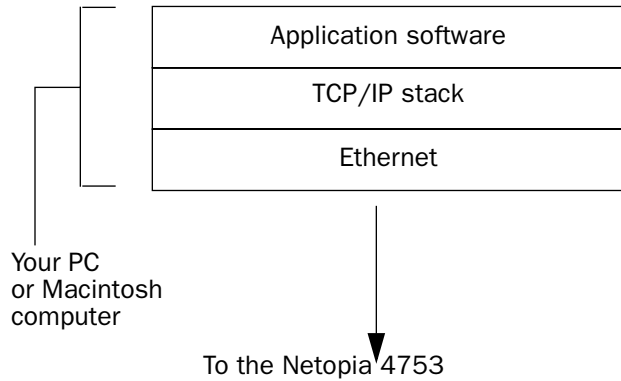
This chapter describes how to physically connect the Netopia 4753 to your local area network (LAN). Before you proceed, make sure the Netopia 4753 is properly configured. You can customize the device's configuration for your particular LAN requirements using console-based management (see [“Console-Based Management” on page 6-1](#)).

This section covers the following topics:

- [“Readying Computers on Your Local Network” on page 5-2](#)
- [“Connecting to an IP and Telephone Network” on page 5-3](#)

Readying Computers on Your Local Network

PC and Macintosh computers must have certain components installed before they can communicate through the Netopia 4753. The following illustration shows the minimal requirements for a typical PC or Macintosh computer.



Application software: This is the software you use to send e-mail, browse the World Wide Web, read newsgroups, etc. These applications may require some configuration. Examples include the Eudora e-mail client and the Web browsers Microsoft Internet Explorer and Netscape Navigator.

TCP/IP stack: This is the software that lets your PC or Macintosh computer communicate using Internet protocols. TCP/IP stacks must be configured with some of the same information you used to configure the Netopia 4753. There are a number of TCP/IP stacks available for PC computers. Windows 95 includes a built-in TCP/IP stack. See [“Configuring TCP/IP on Windows-based Computers” on page 4-2](#). Macintosh computers use either MacTCP or Open Transport. See [“Configuring TCP/IP on Macintosh Computers” on page 4-5](#).

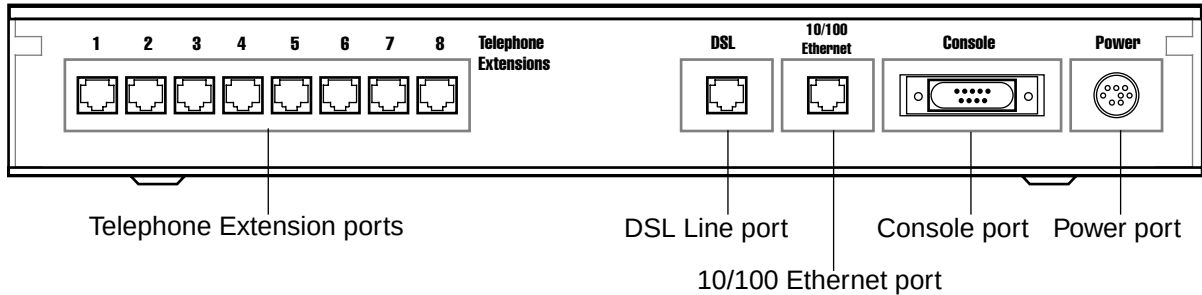
Ethernet: Ethernet hardware and software drivers enable your PC or Macintosh computer to communicate on the LAN.

Once the Netopia 4753 is properly configured and connected to your LAN, PC and Macintosh computers that have their required components in place will be able to connect to the Internet or other remote IP networks.

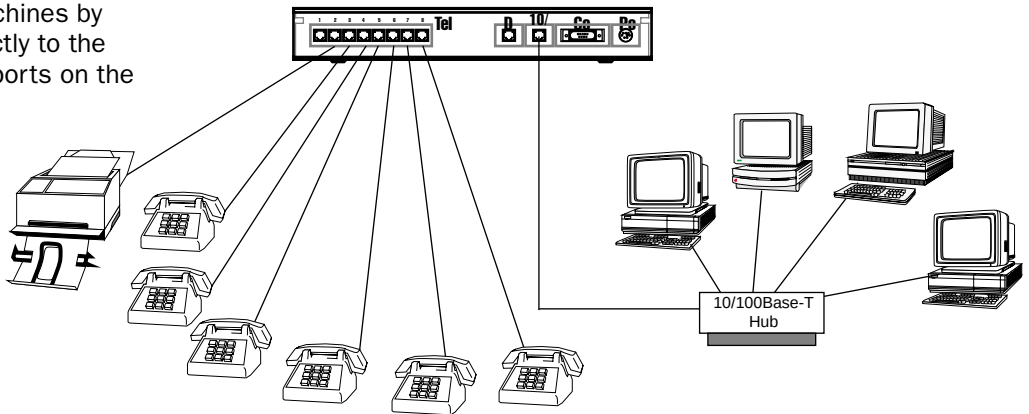
Connecting to an IP and Telephone Network

The Netopia 4753 supports Ethernet connections through its Ethernet port. You can connect a standard 10 or 100Base-T Ethernet network to the Netopia 4753 using its Ethernet port.

Netopia 4753 back panel



Add computers by connecting them to an Ethernet hub and connecting the hub to the Ethernet port on the Netopia 4753. Add telephones or fax machines by connecting them directly to the telephone extension ports on the Netopia 4753.



Note: The Ringer Equivalence Number (REN) is used to determine how many devices can be connected to your telephone line. In most areas, the sum of the REN's of all devices on any one line should not exceed two (2.0). If too many devices are attached, they may not ring properly. The REN for telephone devices is usually listed on the product label or stamped or moulded into the body of the device.

Chapter 6

Console-Based Management

Console-based management is a menu-driven interface for the capabilities built into the Netopia 4753. Console-based management provides access to a wide variety of features that the router supports. You can customize these features for your individual setup. This chapter describes how to access the console-based management screens.

This section covers the following topics:

- “Connecting through a Telnet Session” on page 6-2
- “Connecting a Console Cable to Your Device” on page 6-3
- “Navigating through the Console Screens” on page 6-5

Console-based management screens contain eight entry points to the Netopia 4753 configuration and monitoring features. The entry points are displayed in the Main Menu shown below:

```
Netopia 4753 v5.1

Easy Setup...
WAN Configuration...
System Configuration...
Voice Configuration...
Utilities & Diagnostics...
Statistics & Logs...
Quick Menus...
Quick View...

Return/Enter goes to Easy Setup -- minimal configuration.
You always start from this main screen.
```

- The **Easy Setup** menus display and permit changing the values contained in the default connection profile. You can use Easy Setup to initially configure the router directly through a console session. Easy Setup menus contain up to five descendant screens for viewing or altering these values. The number of screens depends on whether you have optional features installed.
- The **WAN Configuration** menu displays and permits changing your connection profile(s) and default profile, creating or deleting additional connection profiles, and configuring or reconfiguring the manner in which you

6-2 Administration Guide

may be using the router to connect to more than one service provider or remote site.

- The **System Configuration** menus display and permit changing:
 - Internet protocol setup. See [“IP Setup” on page 10-1](#).
 - Filter sets (firewalls). See [“Security” on page 13-1](#).
 - IP address serving. See [“IP Address Serving” on page 10-10](#).
 - Date and time. See [“Date and time \(Network Time Protocol\)” on page 9-17](#).
 - Console configuration. See [“Connecting a Console Cable to Your Device” on page 6-3](#).
 - SNMP (Simple Network Management Protocol). See [“SNMP” on page 14-13](#).
 - Security. See [“Security” on page 13-1](#).
 - Upgrade feature set. See [“Upgrade feature set” on page 9-20](#).
- The **Voice Configuration** menus provide the tools for configuring the voice telephone features available in the Netopia 4753. See [Chapter 8, “Voice Configuration.”](#)
- The **Utilities & Diagnostics** menus provide a selection of seven tools for monitoring and diagnosing the router's behavior, as well as for updating the firmware and rebooting the system. See [“Utilities and Diagnostics” on page 15-1](#) for detailed information.
- The **Statistics & Logs** menus display nine sets of tables and device logs that show information about your router, your network, and their history. See [“Statistics & Logs” on page 14-4](#) for detailed information.
- The **Quick Menus** screen is a shortcut entry point to 22 of the most commonly used configuration menus that are accessed through the other menu entry points.
- The **Quick View** menu displays at a glance current real-time operating information about your router. See [“Quick View Status Overview” on page 14-1](#) for detailed information.

Connecting through a Telnet Session

Features of the Netopia 4753 can be configured through the console screens.

Before you can access the console screens through Telnet, you must have:

- A network connection locally to the router or IP access to the router.

Note: Alternatively, you can have a direct serial console cable connection using the provided console cable for your platform (PC or Macintosh) and the Console port on the back of the router. For more information on attaching the console cable, see [“Connecting a Console Cable to Your Device” on page 6-3](#).

- Telnet software installed on the computer you will use to configure the router

Configuring Telnet software

If you are configuring your router using a Telnet session, your computer must be running a Telnet software program.

- If you connect a PC with Microsoft Windows, you can use a Windows Telnet application or simply run Telnet

from the Start menu.

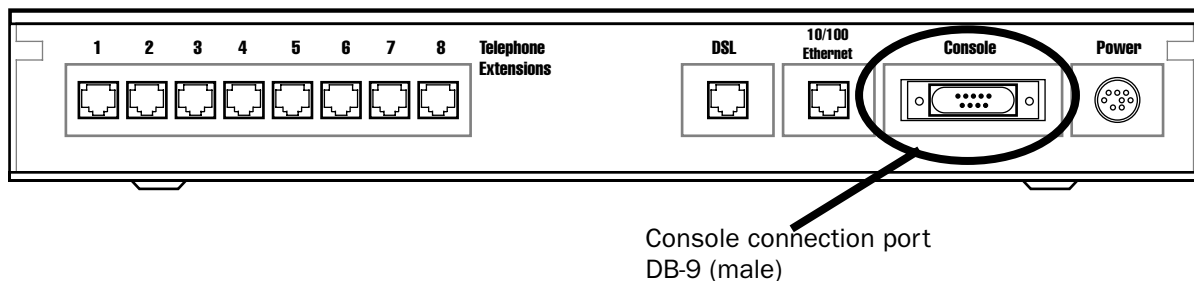
- If you connect a Macintosh computer, you can use the NCSA Telnet program supplied on the Netopia 4753 CD. You install NCSA Telnet by simply dragging the application from the CD to your hard disk.

Connecting a Console Cable to Your Device

You can perform all of the system configuration activities for your Netopia 4753 through a local serial console connection using terminal emulation software, such as HyperTerminal provided with Windows 95, 98, 2000, or NT on the PC, or ZTerm for Classic MacOS or MacOSX, included on the Netopia CD, for Macintosh computers.

The Netopia 4753 back panel has a connector labeled “Console” for attaching the Router to either a PC or Macintosh computer via the serial port on the computer. (On a Macintosh computer, the serial port is called the Modem port or Printer port.) This connection lets you use the computer to configure and monitor the Netopia 4753 via the console screens.

Netopia 4753 back panel



To connect the Netopia 4753 to your computer for serial console communication, use a console cable appropriate to your platform:

- A DB-9 connector end attaches to a PC.
- A mini-DIN8 or a USB connector end attaches to a Macintosh computer depending on your computer's serial bus type. Since Macintosh computers have different serial bus connectors, you will need a mini-DIN8- or USB-to-DB-9 adapter. These are available from a variety of third-party manufacturers.
- A DB-9 end of the Console cable attaches to the Netopia 4753's Console port.
- If you connect a PC with Microsoft Windows 95, 98, 2000 or NT, you can use the HyperTerminal application bundled with the operating system.
- If you connect a Macintosh computer, you can use the ZTerm terminal emulation program on the supplied Netopia 4753 CD.

6-4 Administration Guide

Launch your terminal emulation software and configure the communications software for the values shown in the table below. These are the default communication parameters that the Netopia 4753 uses.

Parameter	Suggested Value
Terminal type	PC: ANSI-BBS Mac: ANSI, VT-100, or VT-200
Data bits	8
Parity	None
Stop bits	1
Speed	9600 bits per second (can be set for up to 57600)
Flow Control	None
Note: The router firmware contains an autobaud detection feature. If you are at any screen on the serial console, you can change your baud rate and press Return (HyperTerminal for the PC requires a disconnect). The new baud rate is displayed at the bottom of the screen.	

Navigating through the Console Screens

Use your keyboard to navigate the Netopia 4753's configuration screens, enter and edit information, and make choices. The following table lists the keys to use to navigate through the console screens.

To...	Use These Keys...
Move through selectable items in a screen or pop-up menu	Up, Down, Left, and Right Arrow
Set a change to a selected item or open a pop-up menu of options for a selected item like entering an upgrade key	Return or Enter
Change a toggle value (Yes/No, On/Off)	Tab
Restore an entry or toggle value to its previous value	Esc
Move one item up	Up arrow or Control + K
Move one item down	Down arrow or Control + O
Display a dump of the device event log	Control + E
Display a dump of the WAN event log	Control + F
Refresh the screen	Control + L

Chapter 7

Easy Setup

This chapter describes how to use the Easy Setup console screens on your Netopia 4753 G.SHDSL Integrated Access Device. After completing the Easy Setup console screens, your device will be ready to connect to the Internet or another remote site.

Easy Setup Console Screens

Using five Easy Setup console screens, you can:

- Modify a connection profile for your device for the connection to your ISP or remote location
- Set up the voice connection to your remote voice provider
- Set up IP addresses and IP address serving
- Password-protect configuration access to your Netopia 4753 G.SHDSL Integrated Access Device

Accessing the Easy Setup console screens

To access the console screens, Telnet to the Netopia 4753 over your Ethernet network or physically connect with a serial console cable and access it with a terminal emulation program. See [“Connecting through a Telnet Session” on page 6-2](#) or [“Connecting a Console Cable to Your Device” on page 6-3](#).

Note: Before continuing, make sure you have the information that your telephone service provider, ISP, or network administrator has given you for configuring the Netopia 4753.

The Netopia 4753's first console screen, Main Menu, appears in the terminal emulation window of the attached PC or Macintosh computer when:

- The Netopia 4753 is turned on
- The computer is connected to the Netopia 4753
- Telnet or the terminal emulation software is running and configured correctly

7-2 Administration Guide

A screen similar to the following Main Menu appears:

```
Netopia 4753 v5.1

Easy Setup...
WAN Configuration...
System Configuration...
Voice Configuration...
Utilities & Diagnostics...
Statistics & Logs...
Quick Menus...
Quick View...

Return/Enter goes to Easy Setup -- minimal configuration.
You always start from this main screen.
```

If you do not see the Main Menu, verify that:

- If you are using a serial connection, that your serial port speed is the same as the Netopia 4753's default 9600 baud, for first use.
- The computer used to view the console screen has its serial port connected to the Netopia 4753's Console port or an Ethernet connection to one of its Ethernet ports. See ["Connecting a Console Cable to Your Device" on page 6-3](#) or ["Connecting through a Telnet Session" on page 6-2](#).
- Telnet or the terminal emulation software is configured for the recommended values.
- If you are connecting via the Console port, your computer's serial port is not being used by another device, such as an internal modem, or an application. Turn off all other programs (other than your terminal emulation program) that may be interfering with your access to the port.
- You have entered the correct password, if necessary. Your Netopia 4753's console access may be password protected from a previous configuration. See your system administrator to obtain the password. See [Appendix A, "Troubleshooting,"](#) for more suggestions.
- If all you see is a pound sign (#), you are in the command line interface. Hit Control-N to exit to the Main Menu.

Quick Easy Setup Connection Path

This section may be all you need to do to configure your Netopia 4753 G.SHDSL Integrated Access Device to connect to the Internet.

Your service provider must supply you with several parameter values for you to enter in the device. The service provider will provide values for the parameters shown below:

Parameter:	Default value:	Your value:
DSL Line Configuration Screen		
Regional Setting	Annex A (default) or Annex B	
Data Link Encapsulation	PPP or RFC1483 (default)	
PPP Mode	VC Multiplexed (default) or LLC SNAP	
RFC1483 Mode	Bridged 1483 (default) or Routed 1483	
PPP over Ethernet (PPPoE) (for Bridged 1483 only)	Off (default) or On	
Data Circuit VPI Data Circuit VPI (for ATM WAN DSL Mode only)	0-255 (8 is default) 0-65535 (35 is default)	
Voice Easy Setup Screen		
Voice Gateway	CopperCom, JetStream, TollBridge, TDSOft or Zhone	
Voice VPI Voice VCI (for any Voice Gateway other than TollBridge)	0-255 (0 is default) 0-65535 (0 is default)	
Easy Setup Profile Screen		
Address Translation Enabled	Yes (default) or No	
IP Addressing	Unnumbered or Numbered (default)	
Local WAN IP Address Local WAN IP Mask	n/a	
Remote IP Address Remote IP Mask	n/a	
PPP Authentication	None (default), PAP or CHAP	
User Name (or Host Name)	n/a	

Parameter:	Default value:	Your value:
Password (or Secret)	n/a	
IP Easy Setup Screen		
Ethernet IP Address	192.168.1.1	
Ethernet Subnet Mask	255.255.255.0	
Domain Name	n/a	
Primary Domain Name Server	n/a	
Secondary Domain Name Server	n/a	
Default IP Gateway	n/a	
Easy Setup Security Configuration Screen		
Write Access Name	n/a	
Write Access Password	n/a	

(If you want to record these values, you can print these pages and use the spaces above.)

If your provider assigns your device a Static IP address, do the following:

1. Open a Telnet session to 192.168.1.1 to bring up the Main Menu.

If you don't know how to do this, see [“Connecting through a Telnet Session” on page 6-2](#).

Alternatively, you can connect the console cable and open a direct serial console connection, using a terminal emulator program. See [“Connecting a Console Cable to Your Device” on page 6-3](#).

The Main Menu appears.

Netopia 4753 v5.1

Easy Setup...

WAN Configuration...

System Configuration...

POTS Configuration...

Utilities & Diagnostics...

Statistics & Logs...

Quick Menus...

Quick View...

Return/Enter goes to Easy Setup -- minimal configuration.
You always start from this main screen.

2. Select the first item on the Main Menu list, **Easy Setup**. Press Return to bring up the DSL Line Configuration menu screen.

DSL Line Configuration

DSL Line Configuration	
Regional Setting...	Annex A
Data Link Encapsulation...	RFC1483
RFC1483 Mode...	Bridged 1483
PPP over Ethernet (PPPoE):	Off
Data Circuit VPI (0-255):	8
Data Circuit VCI (0-65535):	35
PREVIOUS SCREEN	NEXT SCREEN

3. Select **Regional Setting** and from the pop-up menu select either Annex A or Annex B. North American users select Annex A; non-North American users select Annex B.
4. Select **Data Link Encapsulation** and from the pop-up menu choose your DLE.
 - If you selected RFC1483, the next pop-up menu **RFC1483 Mode** offers the choice of Bridged 1483 or Routed 1483. If you select Bridged 1483, a new option **PPP over Ethernet (PPPoE)** appears. You can then toggle PPPoE On or Off. Choosing Routed 1483 hides the PPPoE option.
 - If you selected PPP, the next pop-up menu **PPP Mode** offers the choice of VC Multiplexed or LLC SNAP.
5. The next two fields, **Data Circuit VPI** and **Data Circuit VCI** are editable. Enter the Virtual Path Identifier and Virtual Channel Identifier values that your provider specifies. For more information on VPIs and VCIs, see [“Multiple ATM Permanent Virtual Circuit Support” on page 9-3](#).
6. Press the Down arrow key until you reach **NEXT SCREEN**. Press Return to bring up the next screen.

Voice Easy Setup

Voice Easy Setup

Voice Gateway...

Voice VPI (0-255):

Voice VCI (0-65535):

CopperCom

JetStream

TollBridge

TDSoft

Zhone

PREVIOUS SCREEN

NEXT SCREEN

1. Select **Voice Gateway** and press Return. The pop-up menu will offer you the choice of popular voice gateway devices. Your selection depends on which type your ISP uses: CopperCom, JetStream, TollBridge, TDSoft, or Zhone.
2. For any Voice Gateway other than Tollbridge, the **Voice VPI** and **Voice VCI fields** are editable. (If you select Tollbridge, the VPI and VCI fields do not appear.) Enter the Virtual Path Identifier and Virtual Channel Identifier values that your provider specifies. For more information on VPIs and VCIs, see [“Multiple ATM Permanent Virtual Circuit Support” on page 9-3](#).
3. Press the Down arrow key until you reach **NEXT SCREEN**. Press Return to bring up the next screen.

Easy Setup Profile

The Easy Setup Profile screen is where you configure the parameters that control the Netopia 4753's connection to a specific remote destination, usually your ISP or a corporate site.

On a Netopia 4753 G.SHDSL Integrated Access Device you can add up to 15 more connection profiles, for a total of 16, although, except for Virtual Private Networks, you can only use one at a time.

Connection Profile 1: Easy Setup Profile

Address Translation Enabled:	Yes
IP Addressing...	Numbered
Local WAN IP Address:	0.0.0.0
Remote IP Address:	127.0.0.2
Remote IP Mask:	255.255.255.255
PPP Authentication...	PAP
Send User Name:	jarjar
Send Password:	binks

PREVIOUS SCREEN
NEXT SCREEN

Return accepts * ESC cancels * Left/Right moves insertion point * Del deletes.
Enter basic information about your WAN connection with this screen.

1. To enable address translation, toggle **Address Translation Enabled** to **Yes** (the default). For more information on Network Address Translation, see [Chapter 10, "IP Setup,"](#) on page 10-1.

The **IP Addressing** menu item allows you to choose between Unnumbered and Numbered addressing. Numbered is the default for DSL. It assigns a unique IP address to the DSL WAN interface, as required by most ISPs' routers. Unnumbered may be used for simpler configurations such as point-to-point short haul applications.

2. Select the editable field labeled **Local WAN IP Address**.

The default address is 0.0.0.0, which allows for dynamic addressing, when your ISP assigns an address each time you connect. However, you can enter another specific address if you want to use static addressing. In that case, enter the local WAN address your ISP gave you. Press Return.

3. If you selected PPP data link encapsulation in the DSL Line Configuration screen, a PPP Authentication menu item appears. The authentication protocol and user name/password combinations you enter must be assigned or agreed to in advance between you and your ISP. Select **PPP Authentication** and press Return.

From the pop-up menu that appears, select the authentication method your ISP uses: PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol), or None.

- PAP is the most common, and requires you to enter a User Name and Password in the next two fields.
- CHAP requires you to enter a Host Name and Secret in the next two fields.

4. Press the Down arrow key until you reach **NEXT SCREEN**. Press Return to bring up the next screen.

IP Easy Setup

The IP Easy Setup screen is where you enter information about your Netopia Router's:

- Ethernet IP address
- Ethernet Subnet mask
- Domain Name
- Domain Name Server IP address
- Default gateway IP address

Consult with your network administrator to obtain the information you will need. For more information about setting up IP, see [“IP Setup” on page 10-1](#).

IP Easy Setup

Ethernet IP Address:	192.168.1.1
Ethernet Subnet Mask:	255.255.255.0
Domain Name:	isp.net
Primary Domain Name Server:	209.3.224.21
Secondary Domain Name Server:	209.3.224.20
Default IP Gateway:	127.0.0.2
IP Address Serving:	On
Number of Client IP Addresses:	100
1st Client Address:	192.168.1.100

PREVIOUS SCREEN

NEXT SCREEN

Enter an IP address in decimal and dot form (xxx.xxx.xxx.xxx).
Set up the basic IP & IPX attributes of your Netopia in this screen.

1. Select **Ethernet IP Address** and enter the first IP address from the IP address range your ISP has given you. This will be the Netopia Router's IP address.

The Ethernet IP Address defaults to an address (192.168.1.1) within a range reserved by the Internet address administration authority for use within private networks.

Because this is a private network address, it should never be directly connected to the Internet. Using NAT for all your connection profiles will ensure this restriction. See [“Multiple Network Address Translation” on page 11-1](#) of this guide for more information.

2. Select **Ethernet Subnet Mask** and enter the subnet mask your ISP has given you. The Ethernet Subnet Mask defaults to a standard class mask derived from the class of the Ethernet IP address you entered in the previous step.
3. Press the Down arrow key until the editable field labeled **Domain Name** is highlighted.
4. Type the Domain Name your ISP gave you. Press Return. The next field **Primary Domain Name Server** will be highlighted.

5. Type the Primary Domain Name Server address your ISP gave you. Press Return. A new field **Secondary Domain Name Server** will appear. If your ISP gave you a secondary domain name server address, enter it here. Press Return until the next field **Default IP Gateway** is highlighted.
6. If you do not enter a **Default IP Gateway** value, the router defaults to the remote IP address you entered in the Easy Setup connection profile. If the device does not recognize the destination of any IP traffic, it forwards that traffic to this gateway.

Do not confuse the remote IP address and the Default IP Gateway's address with the block of local IP addresses you receive from your ISP. You use the local IP addresses for the Netopia 4753's Ethernet port and for IP clients on your local network. The remote IP address and the default gateway's IP address should point to your ISP's router.

7. Toggle **IP Address Serving** to On or Off, depending on whether you want the device's IP address server to supply dynamic IP addresses to your client workstations. Normally, you would accept the default On so that workstations on your LAN can use a single IP address assigned by your ISP to connect to the Internet.
8. The IP address server will provide 100 IP addresses automatically to workstations on your LAN. You only need to change the **Number of Client IP Addresses** if you have some other IP addressing scheme.
9. By default, the **1st Client Address** is 192.168.1.100, based on the device's default IP address of 192.168.1.1. You only need to change this if you have some other IP addressing scheme.
10. Press the Down arrow key until you reach **NEXT SCREEN**. Press Return.

Easy Setup Security Configuration

The Easy Setup Security Configuration screen lets you password-protect your Netopia 4753. Input your **Write Access Name** and **Write Access Password** with names or numbers totaling up to eleven digits.

If you password protect the console screens, you will be prompted to enter the name and password you have specified every time you log in to the console screens. Do not forget your name and password. If you do, you will be unable to access any of the configuration screens.

Additional security features are available. See [“Security” on page 13-1](#).

Easy Setup Security Configuration

It is strongly suggested that you password-protect configuration access to your Netopia. By entering a Name and Password pair here, access via serial, Telnet, and SNMP will be password-protected.

Be sure to remember what you have typed here, because you will be prompted for it each time you configure this Netopia.

You can remove an existing Name and Password by clearing both fields below.

Write Access Name:

Write Access Password:

PREVIOUS SCREEN

TO MAIN MENU

RESTART DEVICE

Configure a Configuration Access Name and Password here.

The final step in configuring the Easy Setup console screens is to restart the Netopia 4753, so that the configuration settings take effect.

1. Select **RESTART DEVICE**. A prompt asks you to confirm your choice.
2. Select **CONTINUE** to restart the Netopia Router and have your selections take effect.

Note: You can also restart the system at any time by using the Restart System menu item (see [“Restarting the System” on page 15-12](#)) or by turning the Netopia Router off and on with the power switch.

The Router will restart and your configuration settings will be activated. You can then Exit or Quit your Telnet application.

Easy Setup is now complete.

Chapter 8

Voice Configuration

This chapter describes the telephony services and configuration of the Netopia 4753 G.SHDSL Integrated Access Device. For specific details on configuration and use of the Netopia 4753's Internet connection, refer to [Chapter 7, "Easy Setup"](#) and [Chapter 9, "WAN and System Configuration."](#)

This chapter covers the following topics:

- ["Introduction" on page 8-1](#)
- ["Configuring the Voice Features" on page 8-2](#)

Introduction

The Netopia 4753 provides small and medium sized businesses with a complete Centrex PBX system. It supports voice call switching between the SDSL link and eight local extensions. Call management features can include distinctive ringing, intelligent call forwarding, Direct Inward Dial (DID), Caller ID, and hunt groups. Important key system features such as call hold, call transfer, and call waiting are all supported.

Note: Since the Netopia 4753 is a Centrex-based IAD, specific voice features available to you via the Netopia 4753 will depend on the services for which you contract with your service provider.

The Netopia 4753 supports up to eight telephone extensions and up to eight derived voice lines. Like the rest of the 4700-series line, the Netopia 4753 includes the Netopia data routing engine for any number of attached computers or other network devices connected to a single 10/100 Ethernet port.

Key features include:

- Fax/Modem: Configurable Voice port for incoming fax or modem calls. This is another term for echo cancellation support.
- Voice Gateway Interoperability: CopperCom, JetStream, Tollbridge TDSOft, Zhone. General Bandwidth support to follow in an upcoming firmware release.

Centrex is a simpler variation on the PBX. It is a PBX with all switching occurring at a local telephone office instead of at the company's premises. Typically, the telephone company owns and manages all the communications equipment necessary to implement the PBX and then sells various services to the company.

Explanation of terms

Some telephony terms mean different things in Centrex mode and PBX/local switching mode: Toll Restriction, Speed Dial, and Distinctive Ringing. The Netopia 4753 operates in Centrex mode.

- Toll Restriction Operation - Centrex Mode: When you pick up the phone, you receive a dial tone from the central office. When 9 is pressed, the Netopia 4753 detects 9 and returns a busy tone (locally generated). Incoming calls are allowed. This allows local extension calling through the central office, but not long

8-2 Administration Guide

distance or local calls.

Toll Restriction Operation - PBX/Local Switching Mode: When you pick up the phone, you receive local PBX dial tone. When a 9 (or outside line code) is pressed, the IAD detects the digit and returns busy (locally generated). Incoming calls are allowed. Extension calls (locally switched) are allowed.

- Speed Dial - Centrex Mode: In Centrex Mode, when you pick up the phone, dial-tone from the central office is present. It is therefore, not possible to program the phone or use speed dial in this mode from the phone.

Speed Dial - PBX/Local Switching mode: In this mode, you have the ability to pick up the phone, receive local dial tone and proceed to program the phone w/ local speed dial options. In addition, taking the phone off hook and pressing speed dial numbers will cause the stored speed dial digits to be sent out. This is independent of the previous mode.

Configuring the Voice Features

This section describes how to configure the voice telephone features of the Netopia 4753.

From the Main Menu select **Voice Configuration**.

```
Netopia 4753 v5.1

Easy Setup...
WAN Configuration...
System Configuration...
Voice Configuration...
Utilities & Diagnostics...
Statistics & Logs...
Quick Menus...
Quick View...

Return/Enter goes to Easy Setup -- minimal configuration.
You always start from this main screen.
```

The Voice Configuration screen appears.

Voice Configuration	
Voice Gateway...	CopperCom
Ring Cadence...	20 Hz
Port Configuration...	
Voice Coding...	mu-law
LES Profile Number...	Profile 9

- Select **Voice Gateway** and from the pop-up menu, choose the type of voice gateway device to which you will be connected. The choices are: CopperCom, JetStream, TollBridge, TDSOft, or Zhone.
- Select **Ring Cadence** and press Return. A pop-up menu allows you to choose between 20Hz (the default) and 25Hz for compliance with several non-North American telephone systems.
- Selecting **Port Configuration** displays the Port Configuration screen.

Port Configuration	
Port 1 Echo Cancellation Enabled:	Yes
Compression is	G726 - ADPCM 32K
Port 2 Echo Cancellation Enabled:	Yes
Compression is	G726 - ADPCM 32K
Port 3 Echo Cancellation Enabled:	Yes
Compression is	G726 - ADPCM 32K
Port 4 Echo Cancellation Enabled:	Yes
Compression is	G726 - ADPCM 32K
Port 5 Echo Cancellation Enabled:	Yes
Compression is	G726 - ADPCM 32K
Port 6 Echo Cancellation Enabled:	Yes
Compression is	G726 - ADPCM 32K
Port 7 Echo Cancellation Enabled:	Yes
Compression is	G726 - ADPCM 32K
Port 8 Echo Cancellation Enabled:	Yes
Compression is	G726 - ADPCM 32K

Return/Enter accepts * Tab toggles * ESC cancels.

8-4 Administration Guide

Echo cancellation is set to Yes by default. For ordinary telephone handsets, echo cancellation should be set to Yes (turned on) to eliminate echoes on the voice line. Toggling a port to No allows you to connect a fax machine or modem to the phone port (since fax machines and modems automatically cancel echoes). If you want to disable echo cancellation, toggle this item to **No**. You can enable or disable echo cancellation for each port on the Netopia 4753.

- The **Compression** type is normally set at the voice gateway. It is visible for informational purposes, to ascertain that the provisioning on the voice gateway is in sync with the Netopia 4753.

LES stands for Loop Emulation Service, an increasingly popular standard among ATM voice gateway manufacturers.

If the voice gateway is LES-compliant, a pop-up menu allows you to choose between G711 - PCM 64K and G726 - ADPCM 32K. Your service provider must supply you with the correct provisioning information. The reason is that in those gateway types the voice gateway expects this type of provisioning to be done prior to making any voice calls.

If the voice gateway is not LES-compliant, the pop-up menus are not available, and these fields are for information only.

Once you have made your settings for each voice port, press Escape to return to the Voice Configuration menu.

- Select **Voice Coding** and press Return. From the pop-up menu choose the voice coding method you will be using. The default is mu-law, which is the standard 8-bit, 8 kHz, mono format intended primarily for the requirements of voice in North America. You can also choose a-law, a more common audio format outside North America.
- If your service provider is using an LES-compliant voice gateway, the **LES Profile Number** option becomes visible. From the pop-up menu choose either Profile 9 or Profile 10.

The Netopia 4753 currently supports LES profile 9 and LES profile 10. LES profile 9 includes only PCM calls. LES profile 10 includes PCM and ADPCM capabilities.

Part II: Advanced Configuration

Chapter 9

WAN and System Configuration

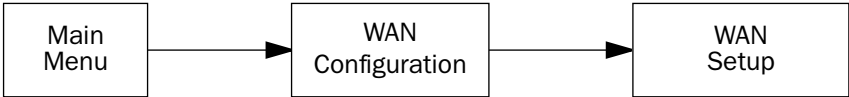
This chapter describes how to use the console-based management screens to access and configure advanced features of your Netopia 4753 G.SHDSL Integrated Access Device. You can customize these features for your individual setup. These menus provide a powerful method for experienced users to set up their device's connection profiles and system configuration.

This section covers the following topics:

- [“WAN Configuration” on page 9-2](#)
- [“Multiple ATM Permanent Virtual Circuit Support” on page 9-3](#)
- [“Creating a New Connection Profile” on page 9-10](#)
- [“The WAN Default Profile” on page 9-13](#)
- [“The ATMP/PPTP Default Profile” on page 9-15](#)
- [“System Configuration Screens” on page 9-15](#)
- [“System Configuration Features” on page 9-16](#)

WAN Configuration

To configure your Wide Area Network (WAN) connection, navigate to the WAN Configuration screen from the Main Menu and select **WAN Configuration**, then **WAN (Wide Area Network) Setup**.



The DSL Line Configuration screen appears.

DSL Line Configuration

Regional Setting...	Annex A
Clock Source...	Network
Cell Format...	Scrambled
Unused Cell Format...	Idle
Data Link Encapsulation...	RFC1483
RFC1483 Mode...	Bridged 1483
PPP over Ethernet (PPPoE):	Off
Display/Change Circuit...	
Add Circuit...	
Delete Circuit...	

Each access concentrator (DSLAM) has a different set of defaults and other parameters.

Your service provider should supply you with the appropriate information about the type and capabilities of the access concentrator equipment they use.

- Select **Regional Setting** and from the pop-up menu select either Annex A or Annex B. North American users select Annex A; non-North American users select Annex B.
- Select **Clock Source** and from the pop-up menu select either Network (the default) or Internal.
- Select **Cell Format** and from the pop-up menu select either Scrambled (the default) or Unscrambled. This setting must match the format used by your service provider. Scrambled is the most common, so you probably do not need to change it unless your provider specifically tells you to do so.
- Select **Unused Cell Format** and from the pop-up menu select either Idle (the default) or Empty. This setting must match the format used by your service provider. Idle is the most common, so you probably do not

need to change it unless your provider specifically tells you to do so.

- Select **Data Link Encapsulation** and from the pop-up menu choose your DLE.
 - If you selected RFC1483, the next pop-up menu **RFC1483 Mode** offers the choice of Bridged 1483 or Routed 1483. If you select Bridged 1483, a new option **PPP over Ethernet (PPPoE)** appears. You can then toggle PPPoE On or Off. Choosing Routed 1483 hides the PPPoE option.
 - If you selected PPP, the next pop-up menu **PPP Mode** offers the choice of VC Multiplexed or LLC SNAP.
- If you selected ATM WAN DSL Mode, the next three fields, **Display/Change Circuit**, **Data Circuit VPI**, and **Data Circuit VCI** are editable. Otherwise they do not appear. Enter the Virtual Path Identifier and Virtual Channel Identifier values that your provider specifies. For more information on VPIs and VCIs, see [“Multiple ATM Permanent Virtual Circuit Support”](#) below.

Multiple ATM Permanent Virtual Circuit Support

The Netopia 4753 supports up to eight permanent virtual circuits.

Multiple ATM PVC overview

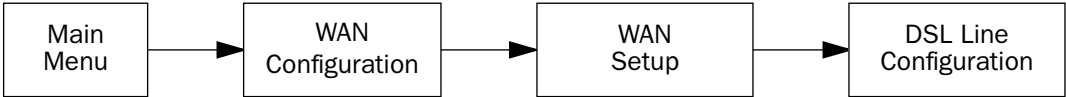
On cell-based DSL WAN interfaces, the ATM connection between the device and the central office equipment (DSLAM) is divided logically into one or more virtual circuits (VCs). A virtual circuit may be either a permanent virtual circuit (PVC) or a switched virtual circuit (SVC). Netopia devices support PVCs.

VCs are identified by a Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI). A VPI is an 8-bit value between 0 and 255, inclusive, while a VCI is a 16-bit value between 0 and 65535, inclusive.

- Circuits now support attributes in addition to their VPI and VCI values. When configuring a circuit, you can specify an optional circuit name of up to 14 characters. The circuit name is used only to identify the circuit for management purposes as a convenience to aid in selecting circuits from lists. The default circuit name is “Circuit <n>”, where <n> is some number between one and eight corresponding to the circuit’s position in the list of up to eight circuits.
- You can also individually enable or disable a circuit without deleting it. This is useful for temporarily removing a circuit without losing the configured attributes.
- In order to function, each circuit must be bound to a Connection Profile or to the Default Profile. Among other attributes, the profile binding specifies the IP addressing information for use on the circuit. Each circuit must be bound to a distinct Connection Profile. You cannot bind multiple circuits to the same Connection Profile.

Multiple ATM PVC configuration

You configure Virtual Circuits in the Add/Change Circuit screen. From the Main Menu, navigate to the DSL Line Configuration screen.



DSL Line Configuration

WAN DSL Mode...	ATM
Regional Setting...	Annex A
Clock Source...	Network
Cell Format...	Scrambled
Unused Cell Format...	Idle
Data Link Encapsulation...	RFC1483
RFC1483 Mode...	Bridged 1483
PPP over Ethernet (PPPoE):	Off
Display/Change Circuit...	
Add Circuit...	
Delete Circuit...	

Select **Display/Change Circuit** and press Return.

Choosing **Display/Change Circuit** (or **Delete Circuit**) displays a pop-up menu that allows you to select the circuit to be modified or deleted.

DSL Line Configuration

WAN DSL Mode...
Regional Setting...

Clock Source...
Cell Format...
Unused Cell Format...

Data Link Encapsulation...
RFC1483 Mode...
PPP over Ethernet (PPPoE):

Display/Change Circuit...
Add Circuit...
Delete Circuit...

ATM
Annex A

Network
Scrambled

+---Circuit Name---VPI/VCI---+

+-----+-----+

Circuit 18/35

Voice Circuit0/0

+-----+-----+

Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Edit.

Changing a circuit

If you want to make any changes to the circuit you select, you make them in the Change Circuit screen.

Change Circuit

Circuit Name:
Circuit Enabled:
Traffic Type...
Circuit VPI (0-255):
Circuit VCI (0-65535):
Connection Profile is

Circuit 1

+-----+

+-----+

Voice

Data

+-----+

38

Easy Setup Profile

- **Circuit Name** allows you to associate a one- to fourteen-character name with the circuit. The default circuit name is “Circuit <n>”, where <n> is some number between one and eight corresponding to the circuit’s position in the list of up to eight circuits.

9-6 Administration Guide

- **Circuit Enabled** allows you to enable or disable the circuit, using the Tab key. The default is enabled.
- **Traffic Type** allows you to select which type of traffic will be routed on this circuit, Voice or Data. If you choose Voice, the *Connection Profile* is field becomes unavailable and does not display.
- **Circuit VPI** allows you to specify the Virtual Path Identifier (VPI) value for the circuit. The default VPI value for both ADSL and cell-based DSL is zero (0).
- **Circuit VCI** allows you to specify the Virtual Channel Identifier (VCI) value for the circuit. The default VCI value depends on the type of DSLAM to which you are connecting.
- Accessing the **Connection Profile Is** field in the Change Circuit menu depends not on the number of Connection Profiles you have created, but the number of *data* VCs you have added. (See [“Adding a circuit” on page 9-7.](#)) If you have more than one data VC you can choose how Connection Profiles are associated with VCs, otherwise you get default behavior and the Connection Profile Is field cannot be selected.

Note: With multiple VCs you must explicitly statically bind the *second* (and all subsequent) VCs to a profile. The first VC will automatically statically bind according to pre-defined dynamic binding rules when you add the second VC. It will revert back to dynamic binding if the number of VCs is reduced to one; for example, by deleting previously defined VCs.

When the link comes up the device binds the VC dynamically to the first suitable Connection Profile or to the Default Profile if there is no Connection Profile configured.

- If you factory default the device, the VC binds to the Default Profile.
- If you delete a Connection Profile that is statically bound to a VC, the VC binding is set back to the Default Profile. If there is only one VC defined, the VC dynamically binds to the first suitable profile or to the Default Profile. If there are multiple VCs defined, it binds to the Default Profile.
- If you add a second VC, it is initialized to the Default Profile, and the menu screens display the VC Connection Profile-related items, allowing you to bind to a specific Connection Profile instead of the Default Profile. In addition, the device statically binds the first VC according to the rules used to select a profile for dynamic binding. At this point, each profile uses static binding when the link is brought up.

If there are no VCs when you add a VC – for example, if you deleted all your previous VCs and started adding them again – dynamic binding will occur when the link comes up. If you delete a VC, leaving only one VC, that VC resumes dynamically binding again.

Adding a circuit

Choosing **Add Circuit** displays the Add Circuit screen.

Add Circuit

Circuit Name:

Circuit 3

Circuit Enabled:

+-----+

Traffic Type...

+-----+
| Voice
| Data
+-----+

Circuit VPI (0-255):

Circuit VCI (0-65535):

0

Use Connection Profile...

Default Profile

Use Default Profile for Circuit

ADD Circuit NOW

CANCEL

The fields in the Add Circuit screen are the similar to the fields in the Change Circuit screen described above. You can add up to seven circuits (for a total of eight) and bind them to separate Connection Profiles.

- **Use Connection Profile** and **Use Default Profile for Circuit** allow you to choose the profile that you want to associate with that circuit. Choosing Use Connection Profile presents a pop-up menu that lists all of your enabled Connection Profiles. Choosing a profile from the list statically binds the circuit to the selected profile. Choosing Use Default Profile for Circuit statically binds the circuit to the Default Profile. When the circuit is bound to a Connection Profile, Use Connection Profile displays the name of the profile; when the circuit is associated with the Default Profile, Use Connection Profile displays Default Profile.

When more than one circuit is enabled, you must explicitly statically bind each circuit to the Connection Profile to be used on the circuit, or to the Default Profile. To do this you use Use Connection Profile or Use Default Profile for Circuit.

To access the ATM VC Statistics screen navigate from the Main Menu to Statistics & Logs then General Statistics.



```

General Statistics
Physical I/F-----Rx Bytes---Tx Bytes---Rx Pkts---Tx Pkts---Rx Err---Tx Err
Ethernet Hub          0          0          0          0          0          0
Aux Async             0          0          0          0          0          0
ATM SDSL 1           22152        5092        403        404          0          0

Network-----Rx Bytes---Tx Bytes---Rx Pkts---Tx Pkts---Rx Err---Tx Err
IP                   0          0          0          0          0          0

VC Traffic Statistics...

```

Select **VC Traffic Statistics**.

The ATM VC Statistics screen appears.

ATM VC Statistics						
VPI/VCI-----	Local IP Addr-----	Frames Rx--	Frames Tx---	Bytes Rx---	Bytes Tx	
-----SCROLL UP-----						
0/39	111.222.333.4	0	0	0	0	
8/36	--	1	0	70	0	
-----SCROLL DOWN-----						

- To display more information about each circuit associated with the selected WAN module, use the up or down arrow key to highlight the circuit you want to view. Press Return.

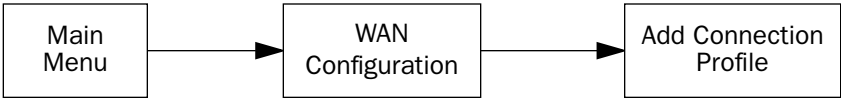
A pop-up window appears, displaying detailed information for the selected circuit.

ATM VC Statistics			
View St+	-----+-----		
VPI/VCI+	-----+-----		
0/39	Circuit Name: Circuit 4		
8/36	Connection Profile Name: Profile 4		
	Bytes Rx:	0	
	Bytes Tx	0	
	Frames Rx:	0	Frames Tx: 0
	Frames Rx Discarded:	0	Frames Tx Discarded: 0
	Errors Rx:	0	
	Errors Tx:	0	
	OK		
	-----+-----		

Creating a New Connection Profile

For a Netopia 4753, connection profiles are useful for configuring the connection and authentication settings for negotiating a PPP connection on the DSL link. If you are using the PPP data link encapsulation method, you can store your authentication information in the connection profile so that your user name and password (or host name and secret) are transmitted when you attempt to connect.

Connection profiles define the networking protocols necessary for the device to make a remote connection. A connection profile is like an address book entry describing how the device is to get to a remote site, or how to recognize and authenticate a connection. To create a new connection profile, you navigate to the WAN Configuration screen from the Main Menu, and select **Add Connection Profile**.



The **Add Connection Profile** screen appears.

Add Connection Profile

Profile Name:

Profile 1

Profile Enabled:

Yes

Data Link Encapsulation...

PPP

Data Link Options...

IP Profile Parameters...

COMMIT

CANCEL

Return accepts * ESC cancels * Left/Right moves insertion point * Del deletes.

Configure a new Conn. Profile. Finished? COMMIT or CANCEL to exit.

On a Netopia 4753 G.SHDSL Integrated Access Device you can add up to 15 more connection profiles, for a total of 16, but you can only use one at a time.

1. Select **Profile Name** and enter a name for this connection profile. It can be any name you wish. For example: the name of your ISP.
2. Toggle **Profile Enabled** to **Yes** or **No**. The default is Yes.

3. Select **Data Link Encapsulation** and press Return. The pop-up menu offers the possible data link encapsulation methods for connection profiles used for a variety of purposes: PPP, RFC1483, ATMP, PPTP, or IPsec. If you select any data link encapsulation method other than RFC1483, a **Data Link Options** menu item is displayed; if you select RFC1483, Data Link Options is hidden.
4. If you chose any data link encapsulation method other than RFC1483 as your data link encapsulation method in the previous step, select **Datalink Options** and press Return. The Datalink Options screen appears.

Datalink (PPP/MP) Options

Data Compression...	Standard LZS
Send Authentication...	PAP
Send User Name:	
Send Password:	
Receive User Name:	
Receive Password:	
Maximum Packet Size:	1500

In this Screen you will configure the PPP/MP specific connection params.

Select **Data Compression** and press Return. The pop-up menu offers the choices of None, Ascend LZS, or Standard LZS. Unless you are otherwise specifically directed, you can accept the default.

Select **Send Authentication** and press Return.

From the pop-up menu that appears, select the authentication method your ISP uses, if any: PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol), or None.

- PAP is the most common, and requires you to enter a User Name and Password in the next two fields.
- CHAP requires you to enter a Host Name and Secret in the next two fields.

You can specify user name and password for both outgoing and incoming connections. the Send User Name/Password parameters are used to specify your identity when connecting to a remote location. The Receive User Name/Password parameters are used when receiving dial-in clients such as via RAS configuration.

5. You can edit the **Maximum Packet Size** field, if you want packets limited to a lower value than 1500. Return to the Add Connection Profile screen by pressing Escape.
6. Select **IP Profile Parameters** and press Return. The IP Profile Parameters screen appears.

IP Profile Parameters

Address Translation Enabled:

Yes

Local WAN IP Address:

0.0.0.0

Remote IP Address:

0.0.0.0

Remote IP Mask:

0.0.0.0

Filter Set...

Remove Filter Set

Receive RIP:

Off

Toggle to Yes if this is a single IP address ISP account.
Configure IP requirements for a remote network connection here.

7. Toggle or enter any IP Parameters you require and return to the Add Connection Profile screen by pressing Escape. For more information, see “IP Setup” on page 10-1.
8. Select **COMMIT** and press Return. Your new Connection Profile will be added.

If you want to view the Connection Profiles in your device, return to the WAN Configuration screen, and select **Display/Change Connection Profile**. The list of Connection Profiles is displayed in a scrolling pop-up screen.

WAN Configuration

+ - Profile Name ----- IP Address ----- +

SmartStart Profile127.0.0.2

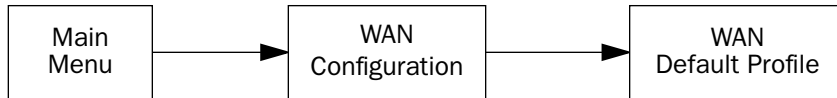
Profile 020.0.0.0

Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Edit.

The WAN Default Profile

If you are using RFC1483 datalink encapsulation, the WAN Default Profile screen controls whether or not the DSL link will come up without an explicitly configured connection profile. (PPP datalink encapsulation does not support a default profile, and the corresponding menu item is unavailable.) See [“Creating a New Connection Profile” on page 9-10](#) for more information.

You access the Default Profile screen from the Main Menu by selecting WAN Configuration and then selecting **Default Profile**.



The Default Profile screen appears.

WAN Default Profile

Must Match a Defined Profile: No

IP Parameters...

Return/Enter accepts * Tab toggles * ESC cancels.
Configure Default WAN Connection Parameters here.

- You can set **Must Match a Defined Profile** item to **Yes** or **No** (the default). This item controls whether or not the DSL link will come up without an explicitly configured connection profile. If your ISP is serving you a dynamic IP Address, you need not explicitly configure a connection profile, and the default behavior of the device will be to connect automatically once it is powered on.
- If you select **IP Parameters** the IP Parameters screen appears (see [“IP Parameters \(Default Profile\) screen” on page 9-14](#)). This screen allows you to configure various IP parameters for DSL connections established without an explicitly configured connection profile.

IP Parameters (Default Profile) screen

If you are using RFC1483 datalink encapsulation, the IP Parameters (Default Profile) screen allows you to configure various IP parameters for DSL connections established without an explicitly configured connection profile:

IP Parameters (Default Profile)

Address Translation Enabled:

No

Filter Set (Firewall)...

Remove Filter Set

Receive RIP:

Both

Transmit RIP:

Off

Return/Enter accepts * Tab toggles * ESC cancels.

For most DSL links, Network Address Translation (NAT) is disabled by default in the Default Profile. You can enable it by toggling to Yes.

If you use RFC1483 as the data link encapsulation method, NAT is enabled by default, as shown below.

IP Parameters (Default Profile)

Address Translation Enabled:

Yes

NAT Map List...

NAT Server List...

Filter Set (Firewall)...

Remove Filter Set

Receive RIP:

Both

For details on setting up IP Parameters see “IP Setup” on page 10-1.

The ATMP/PPTP Default Profile

The ATMP/PPTP Default Profile screen controls whether or not your device will answer VPN connection attempts without an explicitly configured connection profile. See [“Virtual Private Networks \(VPNs\)” on page 12-1](#) for more information.

System Configuration Screens

You can connect to the Netopia 4753's system configuration screens in either of two ways:

- By using Telnet with the device's Ethernet port IP address
- Through the console port, using a local terminal (see [“Connecting a Console Cable to Your Device” on page 6-3](#))

You can also retrieve the Netopia 4753's configuration information and remotely set its parameters using the Simple Network Management Protocol (see [“SNMP” on page 14-13](#)).

Open a Telnet connection to the device's IP address; for example, “192.168.1.1.”

The console screen will open to the Main Menu, similar to the screen shown below:

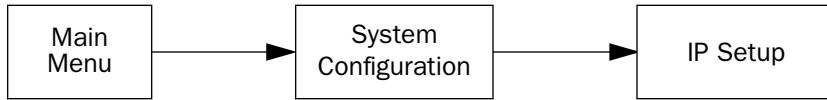
```
Netopia 4753 v5.1

Easy Setup...
WAN Configuration...
System Configuration...
Voice Configuration...
Utilities & Diagnostics...
Statistics & Logs...
Quick Menus...
Quick View...

Return/Enter goes to Easy Setup -- minimal configuration.
You always start from this main screen.
```

Navigating through the System Configuration screens

To help you find your way to particular screens, some sections in this guide begin with a graphical path guide similar to the following example:



This particular path guide shows how to get to the IP Setup screens. The path guide represents these steps:

- Beginning in the Main Menu, select **System Configuration** and press Return. The System Configuration screen appears.
- Select **IP Setup** and press Return. The IP Setup screen appears.

To go back in this sequence of screens, use the Escape key.

System Configuration Features

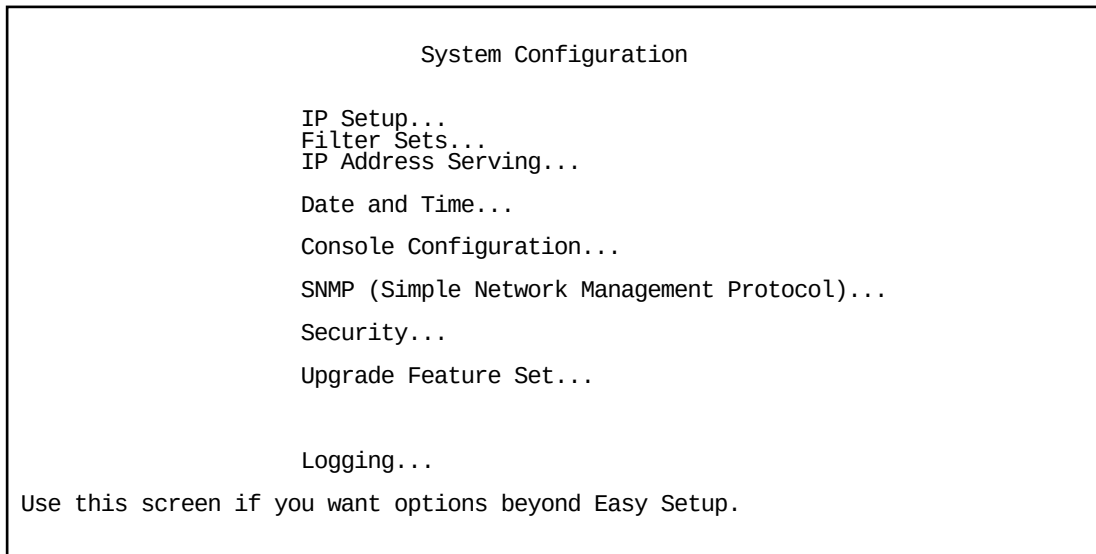
The Netopia 4753 G.SHDSL Integrated Access Device's default settings may be all you need to configure your Netopia 4753. Some users, however, require advanced settings or prefer manual control over the default selections. For these users, the Netopia 4753 provides system configuration options.

To help you determine whether you need to use the system configuration options, review the following requirements. If you have one or more of these needs, use the system configuration options described in later chapters.

- System configuration of dynamic IP address distribution through DHCP or BootP
- Greater network security through the use of filters
- System configuration of connection profiles

To access the system configuration screens, select **System Configuration** in the Main Menu, then press Return.

The System Configuration menu screen appears:



Network protocols setup

These screens allow you to configure your network's use of the standard networking protocols:

- IP: Details are given in [“IP Setup” on page 10-2](#).

Filter sets

These screens allow you to configure security on your network by means of filter sets and a basic firewall.

- Details are given in [“Security” on page 13-1](#).

IP address serving

These screens allow you to configure IP address serving on your network by means of DHCP, WANIP, and BootP.

- Details are given in [“IP Address Serving” on page 10-10](#).

Date and time (Network Time Protocol)

You can set the system's date and time in the Set Date and Time screen.

Select **Date and Time** in the System Configuration screen and press Return. The Set Date and Time screen appears.

Set Date and Time

NTP (Network Time Prot.) Enabled:

On

Time Server Host Name/IP Address

204.152.184.72

Time Zone...

GMT -8:00 Pacific Standard Time

NTP Update Interval (HHHH:MM)

1:00

System Date Format:

MM/DD/YY

System Time Format:

AM/PM

The Netopia 4753 uses Network Time Protocol (NTP) by default to set the date and time automatically. You may want to modify the default settings for your own environment.

NTP takes effect five minutes after the device boots. At that time NTP attempts to connect to a central Time Server and set the device’s clock. If the device is rebooted for any reason, the time settings revert to an internal default date and time for five minutes until NTP can reconnect to its time server and reset the clock.

You should pick a time server close to your location, if possible. Lists of public time servers supported by corporations, governments, and educational institutions are available by searching the Internet.

- Enter a **Time Server Host Name** or **IP Address**. This may be in the form *hostname.domainname* or in dotted quad (*xxx.xxx.xxx.xxx*) notation. The default address 204.152.184.72 is a public NTP server and may be suitable for your needs, or you can supply your own choice.
- From the pop-up **Time Zone** menu, select your time zone.
- Set the **NTP Update Interval** to some convenient interval such as every day (24:00) or every few hours.
- From the pop-up **System Date Format** menu select the date format used in your region: MM/DD/YY, DD/MM/YY, or YY/MM/DD.
- From the pop-up **System Time Format** menu select your preferred time notation: AM/PM or 24hr.

If you do not want to use NTP for date and time setting, you can toggle it to **Off**. In that case, you can set the clock manually (Remember that the clock reverts to a default date and time any time the device is rebooted, so you must reset the clock manually.):

- From the pop-up **System Date Format** menu select the date format used in your region: MM/DD/YY,

DD/MM/YY, or YY/MM/DD.

- Enter the **Current Date** in whatever format you have chosen.
- From the pop-up **System Time Format** menu select your preferred time notation: AM/PM or 24hr.
- Enter the **Current Time** in whatever format you have chosen.
- From the **AM or PM** pop-up menu, select AM or PM.

Console configuration

You can change the default terminal communications parameters to suit your requirements.

To go to the Console Configuration screen, select **Console Configuration** in the System Configuration screen.

Console Configuration

Baud Rate... 57600

SET CONFIG NOW CANCEL

Follow these steps to change a parameter's value:

1. Select the parameter you want to change.
2. Select a new value for the parameter. Return to step 1 if you want to configure another parameter.
3. Select **SET CONFIG NOW** to save the new parameter settings. Select **CANCEL** to leave the parameters unchanged and exit the Console Configuration screen.

SNMP (Simple Network Management Protocol)

These screens allow you to monitor and configure many of the data routing features of your network by means of a standard Simple Network Management Protocol (SNMP) agent.

- Details are given in “SNMP” on page 14-13.

Security

These screens allow you to add users and define passwords on your network.

- Details are given in “Security” on page 13-1.

Upgrade feature set

You can upgrade your Netopia 4753 by adding new feature sets through the Upgrade Feature Set utility.

See the release notes that came with your device or feature set upgrade, or visit the Netopia Web site at www.netopia.com for information on new feature sets, how to obtain them, and how to install them on your Netopia 4753.

Logging

You can configure a UNIX-compatible syslog client to report a number of subsets of the events entered in the device’s WAN Event History. See “WAN Event History” on page 14-5.

The Syslog client (for the PC only) is supplied as a .ZIP file on the Netopia CD.

Select **Logging** from the System Configuration menu.

The Logging Configuration screen appears.

Logging Configuration

WAN Event Log Options

Log Boot and Errors:

Log Line Specific:

Log Connections:

Log PPP, DHCP, CNA:

Log IP:

Yes

Yes

Yes

Yes

Yes

Syslog Parameters

Syslog Enabled:

Hostname or IP Address:

Facility...

No

Local 0

Return/Enter accepts * Tab toggles * ESC cancels.

By default, all events are logged in the event history.

- By toggling each event descriptor to either **Yes** or **No**, you can determine which ones are logged and which are ignored.
- You can enable or disable the syslog client dynamically. When enabled, it will report any appropriate and previously unreported events.
- You can specify the syslog server's address either in dotted decimal format or as a DNS name up to 63 characters.
- You can specify the UNIX syslog Facility to use by selecting the **Facility** pop-up.

Installing the Syslog client

The Goodies folder on the Netopia CD contains a Syslog client daemon program that can be configured to report the WAN events you specified in the Logging Configuration screen.

To install the Syslog client daemon, exit from the graphical Netopia CD program and locate the CD directory structure through your Windows desktop or through Windows Explorer. Go to the Goodies directory on the CD and locate the Sds15000.exe program. This is the Syslog daemon installer. Run the Sds15000.exe program and follow the on-screen instructions for enabling the Windows Syslog daemon.

The following screen shows a sample syslog dump of WAN events:

```
May 5 10:14:06 tsnext.netopia.com Link 1 down: PPP PAP failure
May 5 10:14:06 tsnext.netopia.com >>Issued Speech Setup Request from our DN: 5108645534
May 5 10:14:06 tsnext.netopia.com Requested Disc. from DN: 917143652500
May 5 10:14:06 tsnext.netopia.com Received Clear Confirm for our DN: 5108645534
May 5 10:14:06 tsnext.netopia.com Link 1 down: Manual disconnect
May 5 10:14:06 tsnext.netopia.com >>Issued Speech Setup Request from our DN: 5108645534
May 5 10:14:06 tsnext.netopia.com Requested Disc. from DN: 917143652500
May 5 10:14:06 tsnext.netopia.com Received Clear Confirm for our DN: 5108645534
May 5 10:14:06 tsnext.netopia.com Link 1 down: No answer
May 5 10:14:06 tsnext.netopia.com --Device restarted-----
May 5 10:14:06 tsnext.netopia.com >>Received Speech Setup Ind. from DN: (not supplied)
May 5 10:14:06 tsnext.netopia.com Requested Connect to our DN: 5108645534
May 5 10:14:06 tsnext.netopia.com ASYNC: Modem carrier detected (more) Modem reports: 26400 V34
May 5 10:14:06 tsnext.netopia.com >>WAN: 56K Modem 1 activated at 115 Kbps
May 5 10:14:06 tsnext.netopia.com Connect Confirmed to our DN: 5108645534
May 5 10:14:06 tsnext.netopia.com PPP: Channel 1 up, Answer Profile name: Default Profile
May 5 10:14:06 tsnext.netopia.com PPP: NCP up, session 1, Channel 1 Final (fallback) negotiated
auth: Local PAP , Remote NONE
May 5 10:14:06 tsnext.netopia.com PPP: PAP we accepted remote, Channel 1 Remote name: guest
May 5 10:14:06 tsnext.netopia.com PPP: MP negotiated, session 1 Remote ED0: 06 03 0000C5700624 0
May 5 10:14:06 tsnext.netopia.com PPP: CCP negotiated, session 1, type: Ascend LZS Local mode:
1, Remote mode: 1
May 5 10:14:06 tsnext.netopia.com PPP: BACP negotiated, session 1 Local MN: FFFFFFFF, Remote
MN: 00000001
May 5 10:14:06 tsnext.netopia.com PPP: IPCP negotiated, session 1, rem: 192.168.10.100 local:
192.168.1.1
May 5 10:14:06 tsnext.netopia.com >>WAN: 56K Modem 1 deactivated
May 5 10:14:06 tsnext.netopia.com Received Clear Ind. from DN: 5108645534, Cause: 0
May 5 10:14:06 tsnext.netopia.com Issued Clear Response to DN: 5108645534
May 5 10:14:06 tsnext.netopia.com Link 1 down: Remote clearing
May 5 10:14:06 tsnext.netopia.com PPP: IPCP down, session 1
May 5 10:14:06 tsnext.netopia.com >>Received Speech Setup Ind. from DN: (not supplied)
```


Chapter 10

IP Setup

The Netopia 4753 uses Internet Protocol (IP) to communicate both locally and with remote networks. This chapter shows you how to configure the router to route IP traffic. You also learn how to configure the router to serve IP addresses to hosts on your local network.

Netopia's IP routing features Network Address Translation, Virtual Private Networking (VPNs), and IP address serving.

This section covers the following topics:

- [“IP Setup” on page 10-2](#)
- [“IP Address Serving” on page 10-10](#)
- [“More Address Serving Options” on page 10-17](#)
- [“DHCP Relay Agent” on page 10-23](#)
- [“Connection Profiles” on page 10-25](#)

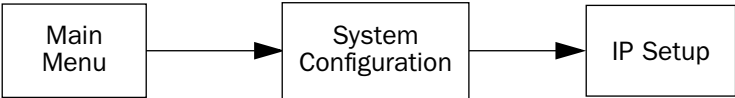
Network Address Translation allows communication between the LAN connected to the Netopia 4753 and the Internet using a single (or a few) IP address(es) instead of a routed account with separate IP addresses for each computer on the network.

Network Address Translation also provides increased security by hiding the local IP addresses of the LAN connected to the Netopia 4753 from the outside world.

The setup is simpler, so ISPs typically offer Internet accounts supporting Network Address Translation at a significant cost savings.

For a detailed discussion of Network Address Translation, see [Chapter 11, “Multiple Network Address Translation.”](#)

IP Setup



The IP Setup options screen is where you configure the Ethernet side of the Netopia 4753. The information you enter here controls how the router routes IP traffic.

Consult your network administrator or ISP to obtain the IP setup information (such as the Ethernet IP address, Ethernet subnet mask, default IP gateway, and Primary Domain Name Server IP address) you will need before changing any of the settings in this screen. Changes to these settings that you make in this screen will take effect only after the Netopia 4753 is reset.

To go to the IP Setup options screen, from the Main Menu, select **System Configuration**, then **IP Setup**.

The IP Setup screen appears.

IP Setup

Ethernet IP Address:	192.128.117.162
Ethernet Subnet Mask:	255.255.255.0
Define Additional Subnets...	
Default IP Gateway:	192.128.117.163
Backup IP Gateway:	0.0.0.0
Primary Domain Name Server:	0.0.0.0
Secondary Domain Name Server:	0.0.0.0
Domain Name:	yourdomain.com
Receive RIP...	Both
Transmit RIP...	Off

Static Routes... IP Address Serving...
Network Address Translation (NAT)... Filter Sets...

Set up the basic IP attributes of your Netopia in this screen.

Follow these steps to configure IP setup for your Netopia 4753:

- Select **Ethernet IP Address** and enter the IP address for the Netopia 4753’s Ethernet port.
- Select **Ethernet Subnet Mask** and enter the subnet mask for the Ethernet IP address that you entered in the last step.
- If you desire multiple subnets select **Define Additional Subnets**. If you select this item you will be taken to the IP Subnets screen. This screen allows you to define IP addresses and masks for additional subnets. See “IP subnets” on page 10-4 for details.

The Netopia 4753 G.SHDSL Integrated Access Device supports multiple IP subnets on the Ethernet interface. You may want to configure multiple IP subnets to service more hosts than are possible with your primary subnet. It is not always possible to obtain a larger subnet from your ISP. For example, if you already have a full Class C subnet, your only option is multiple Class C subnets, since it is virtually impossible to justify a Class A or Class B assignment.

If you are using NAT, you can use the reserved Class A or Class B subnet.

- Select **Default IP Gateway** and enter the IP address for a default gateway. This can be the address of any major router accessible to the Netopia 4753.

A default gateway should be able to successfully route packets when the Netopia 4753 cannot recognize the intended recipient's IP address. A typical example of a default gateway is the ISP's router.
- Select **Primary Domain Name Server** and enter the IP address for a domain name server. The domain name server matches the alphabetic addresses favored by people (for example, robin.hood.com) to the IP addresses actually used by IP routers (for example, 163.7.8.202).
- If a secondary DNS server is available, select **Secondary Domain Name Server** and enter its IP address. The secondary DNS server is used by the Netopia 4753 when the primary DNS server is inaccessible. Entering a secondary DNS is useful but not necessary.
- Select **Domain Name** and enter your network's domain name (for example, netopia.com). Netopia strongly recommends that you enter a domain name.
- Routing Information Protocol (RIP) is needed if there are IP routers on other segments of your Ethernet network that the Netopia 4753 needs to recognize. If this is the case select **Receive RIP** and select **v1**, **v2**, or **Both** from the pop-up menu. With Receive RIP set to v1, the Netopia 4753's Ethernet port will accept routing information provided by RIP packets from other routers that use the same subnet mask. Set to v2, the Netopia 4753 will accept routing information provided by RIP packets from other routers that use different subnet masks. Set to Both, the Netopia 4753 will accept information from either RIP v1 or v2 routers.
- If you want the Netopia 4753 to advertise its routing table to other routers via RIP, select **Transmit RIP** and select **v1**, **v2 (broadcast)**, or **v2 (multicast)** from the pop-up menu. With Transmit RIP v1 selected, the Netopia 4753 will generate RIP packets only to other RIP v1 routers. With Transmit RIP v2 (broadcast) selected, the Netopia 4753 will generate RIP packets to all other hosts on the network. With Transmit RIP v2 (multicast) selected, the Netopia 4753 will generate RIP packets only to other routers capable of recognizing RIP v2 packets.
- Select **Static Routes** to manually configure IP routes. See the section [“Static routes,”](#) below.
- Select **Network Address Translation** to configure advanced MultiNAT features. See [“Multiple Network Address Translation”](#) on page 11-1.
- If you select **IP Address Serving** you will be taken to the IP Address Serving screen (see [“IP Address Serving”](#) on page 10-10). Since no two hosts can use the same IP address at the same time, make sure that the addresses distributed by the Netopia 4753 and those that are manually configured are not the same. Each method of distribution must have its own exclusive range of addresses to draw from.
- If you select **Filter Sets** you will be taken directly to the screen for configuring IP packet filters. For information see [“About Filters and Filter Sets,”](#) beginning on page 13-4.

IP subnets

The IP Subnets screen allows you to configure up to eight Ethernet IP subnets on unlimited-user models, one “primary” subnet and up to seven secondary subnets, by entering IP address/subnet mask pairs:

IP Subnets

	IP Address	Subnet Mask
#1:	192.128.117.162	255.255.255.0
#2:	0.0.0.0	0.0.0.0
#3:		
#4:		
#5:		
#6:		
#7:		
#8:		

Note: You need not use this screen if you have only a single Ethernet IP subnet. In that case, you can continue to enter or edit the IP address and subnet mask for the single subnet on the IP Setup screen.

This screen displays up to eight rows of two editable columns, preceded by a row number between one and eight. If you have eight subnets configured, there will be eight rows on this screen. Otherwise, there will be one more row than the number of configured subnets. The last row will have the value 0.0.0.0 in both the IP address and subnet mask fields to indicate that you can edit the values in this row to configure an additional subnet. All eight row labels are always visible, regardless of the number of subnets configured.

- To add an IP subnet, enter the Netopia 4753’s IP address on the subnet in the **IP Address** field in a particular row and the subnet mask for the subnet in the **Subnet Mask** field in that row.

For example:

IP Subnets		
	IP Address	Subnet Mask
	-----	-----
#1:	192.128.117.162	255.255.255.0
#2:	192.128.152.162	255.255.0.0
#3:	0.0.0.0	0.0.0.0
#4:		
#5:		
#6:		
#7:		
#8:		

- To delete a configured subnet, set both the IP address and subnet mask values to 0.0.0.0, either explicitly or by clearing each field and pressing Return to commit the change. When a configured subnet is deleted, the values in subsequent rows adjust up to fill the vacant fields.

The subnets configured on this screen are tied to the address serving pools configured on the IP Address Pools screen, and changes on this screen may affect the IP Address Pools screen. In particular, deleting a subnet configured on this screen will delete the corresponding address serving pool, if any, on the IP Address Pools screen.

10-6 Administration Guide

If you have configured multiple Ethernet IP subnets, the IP Setup screen changes slightly:

IP Setup

Subnet Configuration...

Default IP Gateway:	192.128.117.163
Primary Domain Name Server:	0.0.0.0
Secondary Domain Name Server:	0.0.0.0
Domain Name:	
Receive RIP...	Both
Transmit RIP...	v2 (multicast)

Static Routes...IP Address Serving...

Network Address Translation (NAT)...

Set up the basic IP attributes of your Netopia in this screen.

The IP address and Subnet mask items are hidden, and the **Define Additional Subnets...** item becomes **Subnet Configuration...**. If you select **Subnet Configuration**, you will return to the IP Subnets screen that allows you to define IP addresses and masks for additional Ethernet IP subnets.

Static routes

Static routes are IP routes that are maintained manually. Each static route acts as a pointer that tells the Netopia 4753 how to reach a particular network. However, static routes are used only if they appear in the IP routing table, which contains all of the routes used by the Netopia 4753 (see [“IP Routing Table” on page 14-9](#)).

Static routes are helpful in situations where a route to a network must be used and other means of finding the route are unavailable. For example, static routes are useful when you cannot rely on RIP.

To go to the Static Routes screen, select **Static Routes** in the IP Setup screen and press Return.

The Static Routes screen will appear.

Static Routes

Display/Change Static Route...

Add Static Route...

Delete Static Route...

Configure/View/Delete Static Routes from this and the following Screens.

Viewing static routes

To display a view-only table of static routes, select **Display/Change Static Route**. The table shown below will appear.

+Dest. Network	---Subnet Mask---	Next Gateway	---Priority	Enabled
0.0.0.0	0.0.0.0	163.176.8.1	Low	Yes

Select a Static Route to modify.

The table has the following columns:

Dest. Network: The network IP address of the destination network.

10-8 Administration Guide

Subnet Mask: The subnet mask associated with the destination network.

Next Gateway: The IP address of the router that will be used to reach the destination network.

Priority: An indication of whether the Netopia 4753 will use the static route when it conflicts with information received from RIP packets.

Enabled: An indication of whether the static route should be installed in the IP routing table.

To return to the Static Routes screen, press Escape.

Adding a static route

To add a new static route, select **Add Static Route** in the Static Routes screen. The Add Static Route screen will appear.

Add Static Route

Static Route Enabled:	Yes
Destination Network IP Address:	0.0.0.0
Destination Network Subnet Mask:	0.0.0.0
Next Gateway IP Address:	0.0.0.0
Route Priority...	High
Advertise Route Via RIP:	No

ADD STATIC ROUTE NOW

CANCEL

Configure a new Static Route in this Screen.

- To install the static route in the IP routing table, select **Static Route Enabled** and toggle it to **Yes**. To remove the static route from the IP routing table, select **Static Route Enabled** and toggle it to **No**.
- Be sure to read the rules on the installation of static routes in the IP routing table. See [“Rules of static route installation” on page 10-9](#).
- Select **Destination Network IP Address** and enter the network IP address of the destination network.
- Select **Destination Network Subnet Mask** and enter the subnet mask used by the destination network.
- Select **Next Gateway IP Address** and enter the IP address for the router that the Netopia 4753 will use to reach the destination network. This router does not necessarily have to be part of the destination network, but it must at least know where to forward packets destined for that network.
- Select **Route Priority** and choose **High** or **Low**. High means that the static route takes precedence over RIP

information; Low means that the RIP information takes precedence over the static route.

- If the static route conflicts with a connection profile, the connection profile will always take precedence.
- To make sure that the static route is known only to the Netopia 4753, select **Advertise Route Via RIP** and toggle it to **No**. To allow other RIP-capable routers to know about the static route, select **Advertise Route Via RIP** and toggle it to **Yes**. When Advertise Route Via RIP is toggled to **Yes**, a new item called **RIP Metric** appears below **Advertise Route Via RIP**.

With RIP Metric you set the number of routers, from 1 to 15, between the sending router and the destination router. The maximum number of routers on a packet's route is 15. Setting **RIP Metric** to **1** means that a route can involve 15 routers, while setting it to **15** means a route can only involve one router.

- Select **ADD STATIC ROUTE NOW** to save the new static route, or select **CANCEL** to discard it and return to the Static Routes screen.
- Up to 32 static routes can be created, but one is always reserved for the default gateway, which is configured using either Easy Setup or the IP Setup screen in system configuration.

Modifying a static route

To modify a static route, in the Static Routes screen select **Display/Change Static Route** to display a table of static routes.

Select a static route from the table and go to the Change Static Route screen. The parameters in this screen are the same as the ones in the Add Static Route screen (see [“Adding a static route” on page 10-8](#)).

Deleting a static route

To delete a static route, in the Static Routes screen select **Delete Static Route** to display a table of static routes. Select a static route from the table and press Return to delete it. To exit the table without deleting the selected static route, press Escape.

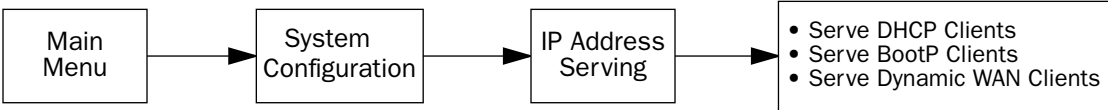
Rules of static route installation

The Netopia 4753 applies certain rules before installing enabled static routes in the IP routing table. An enabled static route will not be installed in the IP routing table if any of the following conditions are true:

- The static route's **Next Gateway IP Address** matches an IP address in the range of IP addresses being distributed by DHCP.
- The static route's **Next Gateway IP Address** is determined to be unreachable by the Netopia 4753.
- The static route's route information conflicts with a connection profile's route information.
- The connection profile associated with the static route has a disabled dial-on-demand setting, and there is no current connection using that connection profile.

A static route that is already installed in the IP routing table will be removed if any of the conditions listed above become true for that static route. However, an enabled static route is automatically reinstalled once the conditions listed above are no longer true for that static route.

IP Address Serving



In addition to being a router, the Netopia 4753 is also an IP address server. There are three protocols it can use to distribute IP addresses.

- The first, called Dynamic Host Configuration Protocol (DHCP), is widely supported on PC networks, as well as Apple Macintosh computers using Open Transport and computers using the UNIX operating system. Addresses assigned via DHCP are “leased” or allocated for a short period of time; if a lease is not renewed, the address becomes available for use by another computer. DHCP also allows most of the IP parameters for a computer to be configured by the DHCP server, simplifying setup of each machine.
- The second, called BootP (also known as Bootstrap Protocol), is the predecessor to DHCP and allows older IP hosts to obtain most of the information that a DHCP client would obtain. However, in contrast, BootP address assignments are “permanent” since there is no lease renewal mechanism in BootP.
- The third protocol, called Dynamic WAN, is part of the PPP/MP suite of wide area protocols used for WAN connections. It allows remote terminal adapters and NAT-enabled routers to be assigned a temporary IP address for the duration of their connection.

Since no two hosts can use the same IP address at the same time, make sure that the addresses distributed by the Netopia 4753 and those that are manually configured are not the same. Each method of distribution must have its own exclusive range of addresses to draw from.

Go to the System Configuration screen. Select **IP Address Serving** and press Return. The IP Address Serving screen will appear.

IP Address Serving

IP Address Serving Mode...	Disabled
Number of Client IP Addresses:	DHCP Server
1st Client Address:	DHCP Relay Agent
Client Default Gateway...	192.168.1.1
Serve DHCP Clients:	Yes
DHCP Lease Time (Hours):	1
DHCP NetBIOS Options...	
Serve BOOTP Clients:	Yes
Serve Dynamic WAN Clients	Yes

Follow these steps to configure IP Address Serving:

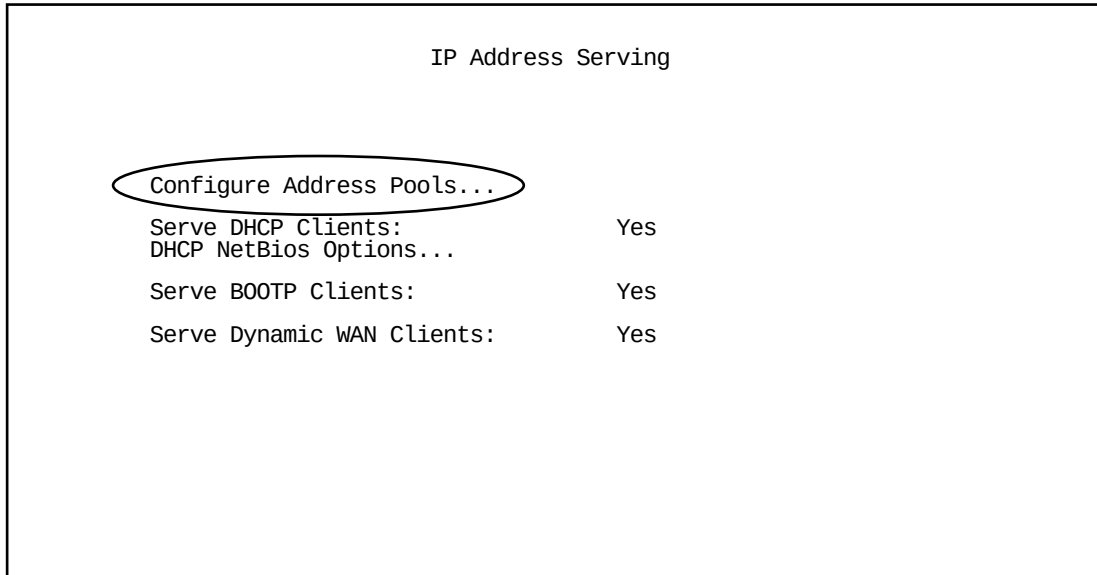
- If you enabled IP Address Serving, then DHCP, BootP clients and Dynamic WAN clients are automatically enabled.
- The **IP Address Serving Mode** pop-up menu allows you to choose the way in which the Netopia 4753 will serve IP addresses. The device can act as either a DHCP Server or a DHCP Relay Agent. (See “[DHCP Relay Agent](#)” on page 10-23 for more information.) In most cases, you will use the device to serve its own pool of IP addresses, hence DHCP Server is the default. Address serving can also be disabled.
- Select **Number of Client IP Addresses** and enter the total number of contiguous IP addresses that the Netopia 4753 will distribute to the client machines on your local area network.
- Select **1st Client Address** and enter the first client IP address that you will allocate to your first client machine. For instance, on your local area network you may want to first figure out which machines are going to be allocated specific static IP addresses so that you can determine the pool of IP addresses that you will be serving addresses from via DHCP, BootP, and/or Dynamic WAN.

Example: Your ISP has given your Netopia 4753 the IP address 192.168.6.137, with a subnet mask of 255.255.255.248. The subnet mask allocated will give you six IP addresses to use when connecting to the ISP over the Internet (for more information on IP addressing refer to [Appendix B, “Understanding IP Addressing.”](#)). Your address range will be from **.137-.142**. In this example you would enter **192.168.6.138** as the 1st Client Address, since the router itself must have an IP address.

- To enable DHCP, select **Serve DHCP Clients** and toggle it to **Yes**. DHCP serving is automatic when IP Address Serving is enabled.
- The default DHCP Lease time is one hour. This may be unnecessarily brief in your network environment. Consequently, the DHCP lease time is now configurable. The **DHCP Lease Time (Hours)** setting allows you to modify the router’s default lease time of one hour. You can enter any number up to and including 168 hours (one week) for the DHCP lease.

10-12 Administration Guide

If you have configured multiple Ethernet IP subnets, the appearance of the IP Address Serving screen is altered slightly:



The first three menu items are hidden, and **Configure Address Pools...** appears instead. If you select **Configure Address Pools...** you will be taken to the IP Address Pools screen that allows you to configure an address serving pool for each of the configured Ethernet IP subnets. See [“IP Address Pools” on page 10-13](#).

IP Address Pools

The IP Address Pools screen allows you to configure a separate IP address serving pool for each of up to eight configured Ethernet IP subnets:

IP Address Pools			
Subnet (# host addrs)	1st Client Addr	Clients	Client Gateway
192.128.117.0 (253)	192.128.117.196	16	192.128.117.162
192.129.117.0 (253)	192.129.117.110	8	192.129.117.4

This screen consists of between two and eight rows of four columns each. There are exactly as many rows as there are Ethernet IP subnets configured on the IP Subnets screen.

- The **Subnet (# host addrs)** column is non-selectable and non-editable. It indicates the network address of the Ethernet IP subnet for which an address pool is being configured and the number of host addresses available on the subnet. The network address is equal to the router's IP address on the subnet bitwise-ANDed with the subnet mask. The host address count is equal to the subnet size minus three, since one address is reserved for the network address, one for the subnet broadcast address, and one for the router's interface address on the subnet.

You can edit the remaining columns in each row.

- The **1st Client Addr** and **Clients** columns allow you to specify the base and extent of the address serving pool for a particular subnet. Entering 0.0.0.0 for the first client address or 0 for the number of clients indicates that no addresses will be served from the corresponding Ethernet IP subnet.
- The Client Gateway column allows you to specify the default gateway address that will be provided to clients served an address from the corresponding pool. The value defaults to the Netopia 4753's IP address on the corresponding subnet (or the Netopia 4753's default gateway, if that gateway is located on the subnet in question). You can override the value by entering any address that is part of the subnet.

DHCP, BootP, and dynamic WAN clients may receive an address from any one of the address serving pools configured on this screen.

10-14 Administration Guide

Numerous factors influence the choice of served address. It is difficult to specify the address that will be served to a particular client in all circumstances. However, when the address server has been configured, and the clients involved have no prior address serving interactions, the Netopia 4753 will generally serve the first unused address from the first address pool with an available address. The Netopia 4753 starts from the pool on the first row and continues to the pool on the last row of this screen.

Once the address server and/or the clients have participated in address serving transactions, different rules apply:

- When requesting an address, a client will often suggest an address to be assigned, such as the one it was last served. The Netopia 4753 will attempt to honor this request if the address is available. The client stores this address in non-volatile storage, for example, on disk, and the specific storage method/location differs depending on the client operating system.
- When requesting an address, a client may provide a client identifier, or, if it does not, the Netopia 4753 may construct a pseudo-client identifier for the client. When the client subsequently requests an address, the Netopia 4753 will attempt to serve the address previously associated with the pseudo-client identifier. This is normally the last address served to the client.
- Otherwise, the Netopia will select the least-recently used available address, starting from the first address in the first pool and ending with the last address in the last pool.

Note: The address serving pools on this screen are tied to the IP subnets configured on the IP Subnets screen. Changes to the IP Subnets screen may affect this screen. In particular, deleting a subnet on the IP Subnets screen will delete the corresponding address serving pool, if any, on this screen.

DHCP NetBIOS Options

If your network uses NetBIOS, you can enable the Netopia 4753 to use DHCP to distribute NetBIOS information.

NetBIOS stands for Network Basic Input/Output System. It is a layer of software originally developed by IBM and Sytek to link a network operating system with specific hardware. NetBIOS has been adopted as an industry standard. It offers LAN applications a variety of “hooks” to carry out inter-application communications and data transfer. Essentially, NetBIOS is a way for application programs to talk to the network. To run an application that works with NetBIOS, a non-IBM network operating system or network interface card must offer a NetBIOS emulator. Many vendors either provide a version of NetBIOS to interface with their hardware or emulate its transport layer communications services in their network products. A NetBIOS emulator is a program provided by NetWare clients that allow workstations to run applications that support IBM's NetBIOS calls.

- Select **DHCP NetBios Options** and press Return. The DHCP NetBIOS Options screen appears.

DHCP NetBios Options

Serve NetBios Type:	Yes
NetBios Type...	Type B
Serve NetBios Scope:	No
NetBios Scope:	
Serve NetBios Name Server:	No
NetBios Name Server IP Addr:	0.0.0.0

Configure DHCP-served NetBIOS options here.

- To serve DHCP clients with the type of NetBIOS used on your network, select **Serve NetBios Type** and toggle it to **Yes**.

- From the **NetBios Type** pop-up menu, select the type of NetBIOS used on your network.

DHCP NetBios Options

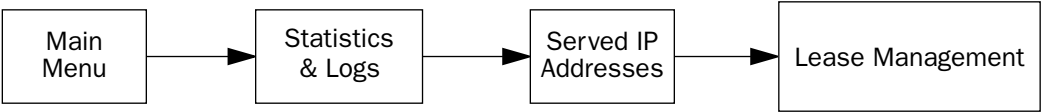
Serve NetBios Type:
NetBios Type...

Serve NetBios Scope:
NetBios Scope:

Serve NetBios Name Server:
NetBios Name Server IP Addr:

+-----+
+-----+
| Type B
| Type P
| Type M
| Type H
+-----+
+-----+
No
0.0.0.0

- To serve DHCP clients with the NetBIOS scope, select **Serve NetBios Scope** and toggle it to **Yes**.
Select **NetBios Scope** and enter the scope.
 - To serve DHCP clients with the IP address of a NetBIOS name server, select **Serve NetBIOS Name Server** and toggle it to **Yes**.
Select **NetBios Name Server IP Addr** and enter the IP address for the NetBIOS name server.
You are now finished setting up DHCP NetBIOS Options. To return to the IP Address Serving screen, press Escape.
 - To enable BootP's address serving capability, select **Serve BOOTP Clients** and toggle to **Yes**.
- Note:** Addresses assigned through BootP are permanently allocated from the IP Address Serving pool until you release them. To release these addresses, navigate back to the Main Menu, then Statistics & Logs, Served IP Addresses, and Lease Management.



IP Address Lease Management

Reset All Leases

Release BootP Leases

Reclaim Declined Addresses

Hit RETURN/ENTER, you will return to the previous screen.

Select **Release BootP Leases** and press Return.

More Address Serving Options

The Netopia 4753 includes a number of enhancements in the built-in DHCP IP address server. These enhancements include:

- The ability to exclude one or more IP addresses from the address serving pool so the addresses will not be served to clients.
- The ability to reserve a particular IP address for a client with a particular Ethernet MAC address.
- The ability to view the host name associated with a client to which the router has leased an IP address.
- The ability for the router's Ethernet IP address(es) to overlap the DHCP address serving pool(s).
- The ability to serve as a DHCP Relay Agent.

The Netopia 4753 supports reserving an IP address only for a type 1 client identifier (i.e., an Ethernet hardware address). It does not support reserving an IP address for an arbitrary client identifier. (For more information on client identifiers, see RFC 2131, section 9.14.)

Configuring the IP Address Server options

To access the enhanced DHCP server functions, from the Main Menu navigate to **Statistics & Logs** and then **Served IP Addresses**.



The following example shows the Served IP Addresses screen after three clients have leased IP addresses. The first client did not provide a Host Name in its DHCP messages; the second and third clients did.

Served IP Addresses			
-IP Address-----	Type----	Expires--	Host Name/Client Identifier-----
-----SCROLL UP-----			
192.168.1.100			
192.168.1.101			
192.168.1.102			
192.168.1.103	DHCP	00:59	EN: 00-00-C5-70-00-04
192.168.1.104	DHCP	00:59	Bill's Pentium
192.168.1.105	DHCP	00:45	Steve's Power Mac
192.168.1.106			
192.168.1.107			
192.168.1.108			
192.168.1.109			
192.168.1.110			
192.168.1.111			
192.168.1.112			
192.168.1.113			
-----SCROLL DOWN-----			
Lease Management...			

The rightmost column displays the host name supplied by the client if one was provided; otherwise it displays the client identifier. (If a host name is displayed, the client identifier is still accessible in a Details pop-up menu. See below.)

Note: The server does not query the client for its host name. Macintosh computers running versions of MacOS prior to MacOS version 8.5 (OT 2.0.1, TCP/IP 2.0.1) do not supply a host name option in their DHCP messages, so no host name will appear in the Served IP Addresses list.

You can select the entries in the Served IP Addresses screen. Use the up and down arrow keys to move the selection to one of the entries in the list of served IP addresses.

Served IP Addresses			
-IP Address-----	Type----	Expires--	Host Name/Client Identifier-----
-----SCROLL UP-----			
192.168.1.100			
192.168.1.101			
192.168.1.102			
192.168.1.103			
192.168.1.104			
192.168.1.105			
192.168.1.106	+-----+		
192.168.1.107	+-----+		
192.168.1.108	Details...		Barr's XPi 120
192.168.1.109	Exclude		
192.168.1.110	Release		
192.168.1.111	Reserve...		
192.168.1.112	+-----+		
192.168.1.113			
-----SCROLL DOWN-----			
Lease Management...			

Once you select an entry, pressing Return displays an action pop-up menu that lists operations that can be performed on that entry. Possible operations are **Details...**, **Exclude**, **Include**, **Release**, and **Reserve...** The action popup is context-sensitive and lists only those operations that apply to the selected IP address in its current lease state.

- **Details...** is displayed if the entry is associated with both a host name and a client identifier.

Selecting **Details...** displays a pop-up menu that provides additional information associated with the IP address. The pop-up menu includes the IP address as well as the host name and client identifier supplied by the client to which the address is leased.

Served IP Addresses

-IP Address-----Type----Expires--Host Name/Client Identifier-----

-----SCROLL UP-----

192.168.1.100

192.168.1.101

+-----+-----+-----+-----+

+-----+-----+-----+-----+

IP Address is 192.168.1.108

Host Name is Barr's XPi 120

Client ID is EN: 00-00-c5-45-89-ef

OK

+-----+-----+-----+-----+

192.168.1.111 | Reserve... |

192.168.1.112 +-----+

192.168.1.113

-----SCROLL DOWN-----

Lease Management...

- **Exclude** is displayed if the entry is not already excluded.

Selecting **Exclude** excludes the IP address from the address serving pool so the address will not be served to a client. If the IP address is currently leased to or reserved for a client, you will be presented with a warning dialog asking you to confirm the operation.

Served IP Addresses			
-IP Address-----	Type----	Expires--	Host Name/Client Identifier-----
-----SCROLL UP-----			
192.168.1.100			
192.168.1.101			
192.1+	-----+-----		
192.1+	-----+-----		
192.1	You are about to make changes that will affect an address		
192.1	that is currently in use. Are you sure you want to do this?		
192.1			
192.1	CANCEL		OK
192.1	-----+-----		
192.1+	-----+-----		
192.168.1.111	Reserve...		
192.168.1.112	+-----+		
192.168.1.113			
-----SCROLL DOWN-----			
Lease Management...			

- **Include** is displayed if the entry is either excluded or declined.

An IP address is marked declined when a client to whom the DHCP server offers the address declines the address. A client declines an address if it determines that a leased address is already in use by another device.

Selecting **Include** restores the selected IP address to the address serving pool so that the IP address is once again eligible to be served to a client.

- **Release** is displayed if the entry is currently offered, leased, or reserved.

Selecting **Release** puts the selected entry in the available state. You will be presented with a warning dialog asking you to confirm the operation since the IP address is in use. There is no mechanism to notify the client to whom the address is leased that the lease has been terminated. Thus, the client will continue to use the address until the next time it attempts to renew its lease. In the interim, the server may lease the same IP address to a different client, thereby creating an address conflict. For this reason, releasing an address that is actively being used by a client is generally not recommended.

- **Reserve...** is displayed if the entry is available, declined, excluded, leased, offered, or reserved.

Reserving an IP address for a client with a particular Ethernet MAC address guarantees that a client with the specified MAC address will be offered or leased the specified IP address. Moreover, it prevents the specified IP address from being offered or leased to any other client.

Selecting **Reserve...** displays a pop-up dialog box that displays the IP address and editable item in which you can enter an Ethernet MAC address. The pop-up dialog box includes **OK** and **CANCEL** buttons for confirming or cancelling the operation. If the IP address is currently offered or leased to, or reserved for, a client, you will be presented with a warning dialog asking you to confirm the operation. Reserving an IP address guarantees that the IP address will only be leased.

```

Served IP Addresses
-IP Address-----Type----Expires--Host Name/Client Identifier-----
-----SCROLL UP-----
192.168.1.100
192.168.1.101
192.168.1.102
192.168.1.103
192.168.1.104
192.168.1.105
192.168.1.106
192.168.1.107
192.168.1.108
192.168.1.109
192.168.1.110
192.168.1.111
192.168.1.112
192.168.1.113
-----SCROLL DOWN-----
Lease Management...
```

IP Address is 192.168.1.108
MAC Address: 00-00-c5-45-89-ef

CANCEL OK

The router’s Ethernet IP address(es) will be automatically excluded from the address serving pool(s) on startup. Entries in the served IP address list corresponding to the router’s Ethernet IP address(es) that have been automatically excluded on startup are not selectable.

```

Served IP Addresses
-IP Address-----Type----Expires--Host Name/Client Identifier-----
-----SCROLL UP-----
192.168.1.1      Excluded for the router's IP address
192.168.1.2      Excluded
192.168.1.3      DHCP      00:24      Barr's XPi 120
192.168.1.4
192.168.1.5
192.168.1.6
192.168.1.7
192.168.1.8
192.168.1.9
192.168.1.10
192.168.1.11
192.168.1.12
192.168.1.13
192.168.1.14
-----SCROLL DOWN-----
Lease Management...

Hit RETURN/ENTER for available operations.
```

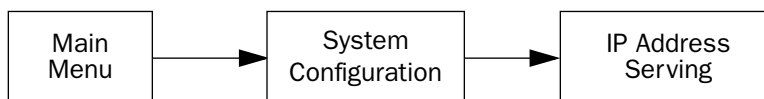
DHCP Relay Agent

The Netopia 4753 offers DHCP Relay Agent functionality, as defined in RFC1542. A DHCP relay agent is a computer system or a router that is configured to forward DHCP requests from clients on the LAN to a remote DHCP server, and to pass the replies back to the requesting client systems.

When a DHCP client starts up, it has no IP address, nor does it know the IP address of a DHCP server. Therefore, it uses an IP broadcast to communicate with one or more DHCP servers. These broadcasts are normally limited to the network segment on which the client is located, and do not pass through routers such as the Netopia Router. If the Netopia Router is configured to act as a DHCP server, it will assign the client an address from an address pool configured locally in the Netopia Router and respond to the client's request itself.

However, if the Netopia Router is configured to act as a DHCP relay agent, it does not satisfy the DHCP request itself, but instead forwards the request to one or more remote DHCP servers. These servers process the request, assign an address from an address pool configured on the remote server, and forward the response back to the Netopia Router for delivery back to the client. The agent then sends the response to the client on behalf of the DHCP server. This process is transparent to the client, which doesn't know that it is communicating through an intermediary rather than directly to a local server. Using DHCP relay, it is possible to centralize the configuration information for the host computers at many remote sites at a single location, easing the burden of administering configuration management for remote sites.

To configure the Netopia Router to act as a DHCP relay agent, from the Main Menu navigate to the System Configuration menu.



10-24 Administration Guide

Select **IP Address Serving** and press Return. The IP Address Serving screen appears.

```

                                IP Address Serving
                                +-----+
                                |         |
IP Address Serving Mode...    | Disabled |
                                | DHCP Server |
Number of Client IP Addresses: | DHCP Relay Agent |
1st Client Address:           |         |
Client Default Gateway...     | 192.168.1.1 |
                                +-----+

Serve DHCP Clients:           Yes
DHCP NetBIOS Options...

Serve BOOTP Clients:         Yes

```

Select **IP Address Serving Mode**. The pop-up menu offers the choices of **Disabled**, **DHCP Server** (the default), and **DHCP Relay Agent**.

If you select DHCP Relay Agent and press Return, the screen changes as shown below.

```

                                IP Address Serving

IP Address Serving Mode...    DHCP Relay Agent

Relay Server #1:             10.1.1.1
Relay Server #2:             20.1.1.1
Relay Server #3:             30.1.1.1

Configure Address Serving (DHCP, BOOTP, etc.) here.

```

Now you can enter the IP address(es) of your remote DHCP server(s), such as might be located in your company's corporate headquarters. Each time you enter an IP address and press Return, an additional field appears. You can enter up to four DHCP server addresses.

In the example above, DHCP requests from clients on the LAN will be relayed to the DHCP servers at IP addresses 10.1.1.1, 20.1.1.1, and 30.1.1.1.

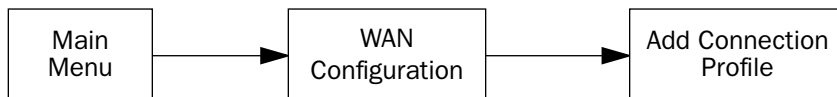
Note: The remote DHCP server(s) to which the Netopia Router is relaying DHCP requests must be capable of servicing relayed requests. Not all DHCP servers support this feature. For example, the DHCP server in the Netopia Router does *not*.

The DHCP server(s) to which the Netopia Router is relaying DHCP requests must be configured with one or more address pools that are within the Netopia Router's primary Ethernet LAN subnet. (There is no mechanism for DHCP clients to receive an address on a secondary subnet via a relayed DHCP request.)

Connection Profiles

Since you will probably only have a single connection to your ISP over the DSL link, you may not need to create multiple connection profiles. Additional profiles may be useful for creating VPNs.

Connection Profiles define the line and networking protocols necessary for the router to make a remote connection. A connection profile is like an address book entry describing how the router is to get to a remote site, or how to recognize and authenticate a remote user connecting to the router. To create a new Connection Profile, you navigate to the WAN Configuration screen from the Main Menu, and select **Add Connection Profile**.



The Add Connection Profile screen appears.

Add Connection Profile

Profile Name:	Profile 1
Profile Enabled:	Yes
Data Link Encapsulation...	PPP
Data Link Options...	
IP Profile Parameters...	
COMMIT CANCEL	

Configure a new Conn. Profile. Finished? COMMIT or CANCEL to exit.

On a Netopia 4753 G.SHDSL Integrated Access Device you can add up to 15 more connection profiles, for a total of 16, although only one can be used at a time, unless you are using VPNs.

10-26 Administration Guide

1. Select **Profile Name** and enter a name for this connection profile. It can be any name you wish. For example: the name of your ISP.
2. Toggle the **Profile Enabled** value to **Yes** or **No**. The default is Yes.
3. Select **IP Profile Parameters** and press Return. The IP Profile Parameters screen appears.

IP Profile Parameters

Address Translation Enabled:	Yes
IP Addressing...	Numbered
NAT Map List...	Easy-PAT List
NAT Server List...	Easy-Servers
Local WAN IP Address:	0.0.0.0
Local WAN IP Mask:	0.0.0.0
Remote IP Address:	0.0.0.0
Remote IP Mask:	0.0.0.0
Filter Set...	
Remove Filter Set	
RIP Profile Options...	

Configure IP requirements for a remote network connection here.

4. Toggle or enter any IP parameters you require and return to the Add Connection Profile screen by pressing Escape. For more information on NAT, see [“Multiple Network Address Translation,” beginning on page 11-1](#). For more information on IP addressing, see [Appendix B, “Understanding IP Addressing.”](#)

The Local WAN IP Address is displayed for numbered or NAT profiles. The Local WAN IP Mask is displayed for numbered profiles. The Remote IP Address and Remote IP Mask are displayed for unnumbered profiles.

5. Select **ADD PROFILE NOW** and press Return. Your new connection profile will be added.

If you want to view the connection profiles in your router, return to the WAN Configuration screen, and select **Display/Change Connection Profile**. The list of connection profiles is displayed in a scrolling pop-up screen.

WAN Configuration

+ - Profile Name - - - - -	IP Address - - - - -
Easy Setup Profile	127.0.0.2
Profile 1	0.0.0.0

on: Yes

Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Edit.

Chapter 11

Multiple Network Address Translation

The Netopia 4753 offers advanced Multiple Network Address Translation functionality.

You should read this chapter completely before attempting to configure any of the advanced NAT features.

This chapter covers the following topics:

- [Overview on page 11-1](#)
- [MultiNAT Configuration on page 11-6](#)
- [Easy Setup Profile configuration on page 11-6](#)
- [Server Lists and Dynamic NAT configuration on page 11-6](#)
- [Adding Server Lists on page 11-17](#)
- [Binding Map Lists and Server Lists on page 11-23](#)
- [NAT Associations on page 11-27](#)
- [MultiNAT Configuration Example on page 11-29](#)

Overview

NAT (Network Address Translation) is a means of mapping one or more IP addresses and/or IP service ports into different values. This *mapping* serves two functions:

- It allows the addresses of many computers on a LAN to be represented to the public Internet by only one or a few addresses, saving you money.
- It can be used as a security feature by obscuring the true addresses of important machines from potential hackers on the Internet.

To help you understand some of the concepts discussed here, it may be helpful to introduce some NAT terminology.

The term *mapping* refers to rules that associate one or more private addresses on the Netopia Router's LAN to one or more public addresses on the Netopia Router's WAN interface (typically the Internet).

The terms *private* and *internal* refer to addresses on the Netopia Router's LAN. These addresses are considered private because they are protected or obscured by NAT and cannot be directly accessed from the WAN (or Internet) side of the Netopia Router unless specifically configured otherwise.

The terms *public* and *external* refer to the WAN (or Internet) side of the Netopia Router.

Features

MultiNAT features can be divided into several categories that can be used simultaneously in different combinations on a per-Connection Profile basis.

The following is a general description of these features:

Port Address Translation

The simplest form of classic Network Address Translation is *PAT* (Port Address Translation). PAT allows a group of computers on a LAN, such as might be found in a home or small office, to share a single Internet connection using one IP address. The computers on the LAN can surf the Web, read e-mail, download files, etc., but their individual IP addresses are never exposed to the public network. Instead, a single IP address acts as the source IP address of traffic originating from the LAN. The Netopia Router allows you to define multiple PAT mappings, which can be individually mapped to different public IP addresses. This offers more control over the access permitted to users on the LAN.

A limitation of PAT is that communication must be initiated from the internal network. A user on the external side cannot access a machine behind a PAT connection. A PAT enhancement introduced in firmware version 4.4 is the ability to define multiple PAT mappings. Each of these can optionally map to a section or *range* of IP addresses of the internal network. PAT mapping allows only internal users to initiate traffic flow between the internal and external networks.

Server lists

Server lists, previously known as exported services, make it possible to provide access from the public network to hosts on the LAN. Server lists allow you to define particular services, such as Web, ftp, or e-mail, which are available via a public IP address. You define the type of service you would like to make available and the internal IP address to which you would like to provide access. You may also define a specific public IP address to use for this service if you want to use an IP other than the WAN IP address of the Netopia Router.

Static mapping

If you want to host your own Website or provide other Internet services to the public, you need more than classic NAT. The reason is noted under Port Address Translation above – external users cannot initiate traffic to computers on your LAN because external users can never see the real addresses of the computers on your LAN. If you want users outside your LAN to have access, for example, to a Web or FTP server that you host, you need to make a public representation of the real IP addresses of those servers.

Static mappings are a way to make one or more private IP addresses fully accessible from the public network via corresponding public IP addresses. Some applications may negotiate multiple TCP connections in the process of communication, which often does not work with traditional PAT. Static mapping offers the ability to use these applications through NAT. Each private IP address is mapped, on a one-to-one basis, to a public IP address that can be accessed from the Internet or public network. As with PAT mappings, you may have multiple static mappings to map a range of private IP addresses to a range of public IP addresses if desired.

Dynamic mapping

Dynamic mapping, often referred to as many-to-few, offers an extension to the advantages provided by static mapping. Instead of requiring a one-to-one association of public addresses and private addresses, as is required in static mapping, dynamic mapping uses a group of public IP addresses to dynamically allocate static mappings to private hosts that are communicating with the public network. If a host on the private network initiates a connection to the Internet, for example, the Netopia Router automatically sets up a one-to-one mapping of that host's private IP address to one of the public IP addresses allocated to be used for Dynamic NAT. As long as this host is communicating with the Internet, it will be able to use that address. When traffic from that host ceases, and no traffic is passed from that host for five minutes, the public address is made available again for other private hosts to use as necessary.

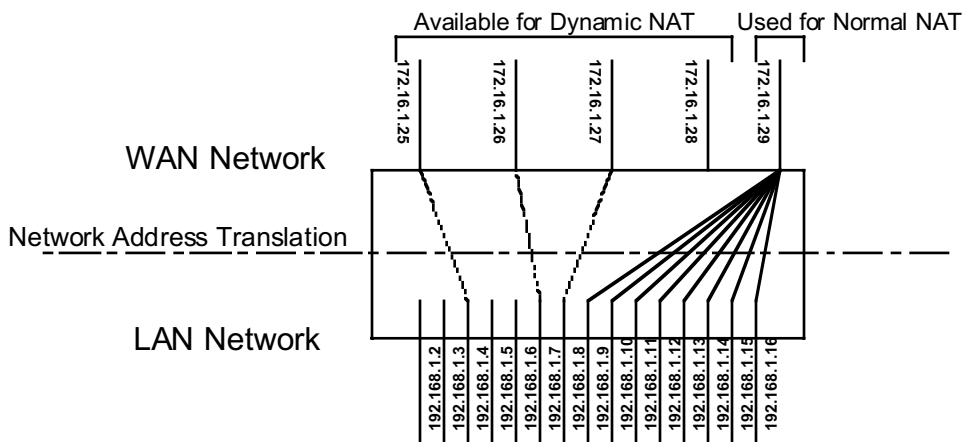
When addresses are returned to the group of available addresses, they are returned to the head of the group, being the most recently used. If that same host requests a connection an hour later, and the same public address is still available, then it will be mapped to the same private host. If a new host, which has not previously requested a connection, initiates a connection it is allocated the last, or oldest, public address available.

Dynamic NAT is a way of sharing a range of public, or exterior, NAT addresses among one or more *groups* of private, or interior, hosts. This is intended to provide superior support for applications that traditionally have difficulty communicating through NAT. Dynamic NAT is intended to provide functionality beyond many-to-one and one-to-one translation. Netopia's NAT implementation makes it possible to have a static mapping of one public address to one private address, thus allowing applications such as NetMeeting to work by assuring that any traffic sent back to the source IP address is forwarded through to the internal machine.

Static one-to-one mapping works well if you have enough IP addresses for all the workstations on your LAN. If you do not, Dynamic NAT allows machines to make full use of the publicly routable IP addresses provided by the ISP as necessary, on demand. When these public IP addresses are no longer being used by a particular workstation, they are returned to a pool of available addresses for other workstations to use.

A common example is a DSL customer's application. Most DSL ISPs only provide customers with a few IP addresses for use on their network. For networks with more than four or five machines it is usually mandatory to use NAT. A customer may have 15 workstations on the LAN, all of which need Internet access. The customer is only provided five IP addresses by their ISP. The customer has eight hosts, which only need to use email and have Web access, but another seven hosts, which use NetMeeting to communicate with clients once or twice a day. NetMeeting will not work unless a static one-to-one mapping exists for the machine running NetMeeting to use for communication. The customer does not have enough IP addresses to create a one-to-one mapping for each of the seven users. This is where dynamic NAT applies.

The customer can configure four of these addresses to be used for Dynamic NAT. The fifth address is then used for the eight other machines that do not need one-to-one mappings. As each machine configured to use addresses from the dynamic pool tries to connect to the Internet it is allocated a public IP address to use temporarily. Once the communication has been terminated, that IP address is freed for one of the other six hosts to use.



Exterior addresses are allocated to internal hosts on a demand, or as-needed, basis and then made available when traffic from that host ceases. Once an internal host has been allocated an address, it will use that address for all traffic. Five minutes after all traffic ceases – no pings, all TCP connections closed, no DNS requests, etc. – the address is put at the head of an *available* list. If an interior host needs an exterior address an hour later, and the previously used address is still available, it will acquire the same address. If an interior host that has not previously been allocated an exterior address needs one, it will be allocated the last, hence the oldest, exterior address on the available list.

All NAT configurations are *rule-based*. This means that traffic passed through NAT from either the public or the private network is compared to the rules and mappings configured in the Netopia Router in a particular order. The first rule that applies to the traffic being initiated is used.

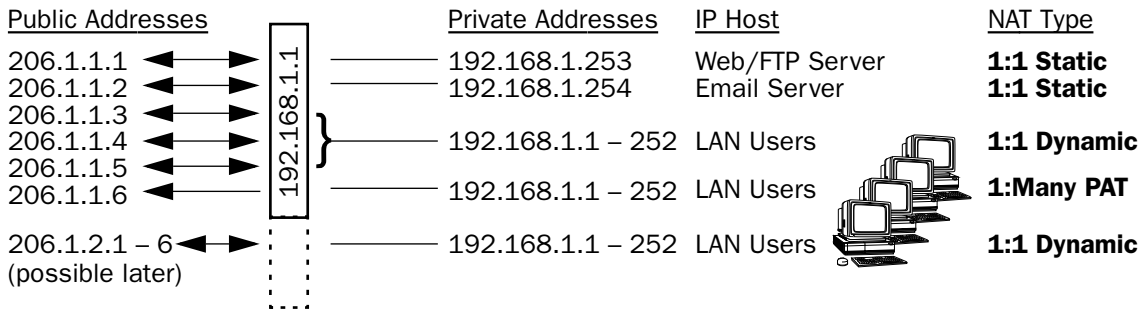
For example, if a connection is initiated from the public network and is destined for a public IP address configured on the Netopia Router, the following comparisons are made in this order.

1. The Netopia Router first checks its internal NAT cache to see if the data is part of a previously initiated connection, if not...
2. The Netopia Router checks the configured server lists to see if this traffic is intended to be forwarded to an internal host based on the type of service.
3. The Netopia Router then checks to see if there is a static, dynamic, or PAT mapping for the public IP address that the connection is being initiated to.
4. The Netopia Router answers the request itself if the data is destined for the Netopia’s WAN interface IP address. Otherwise the data is discarded.

Complex maps

Map lists and server lists are completely independent of each other. A Connection Profile can use one or the other or both.

MultiNAT allows complex mapping and requires more complex configuration than in earlier firmware versions. Multiple mapped interior subnets are supported, and the rules for mapping each of the subnets may be different. The figure below illustrates a possible multiNAT configuration.



In order to support this type of mapping, you define two address ranges. First, you define a public range which contains the first and last public address to be used and the way in which these addresses should be used (PAT, static, or dynamic). You then configure an address map which defines the private IP address or addresses to be used and which public range they should be mapped to. You add the address map to the list of address maps which are configured, creating a map list. The mappings in the map list are order-dependent and are compared in order from the top of the list to the bottom. If a particular resource is not available, subordinate mappings can be defined that will redirect traffic.

Supported traffic

MultiNat supports the following IP protocols:

- PAT: TCP/UDP traffic which does not carry source or destination IP addresses or ports in the data stream (i.e., HTTP, Telnet, 'r' commands, tftp, NFS, NTP, SMTP, NNTP, etc.).
- Static NAT: All IP protocol traffic which does not carry or otherwise rely on the source or destination IP addresses in the data stream.
- Dynamic NAT: All IP protocol traffic which does not carry or otherwise rely on the source or destination IP addresses in the data stream.

MultiNAT Configuration

You configure the MultiNAT features through the console menu:

- For a simple 1-to-many NAT configuration (classic NAT or PAT), use the [Easy Setup Profile configuration](#), described below.
- For the more advanced features, such as server lists and dynamic NAT, follow the instructions in:
 - [IP setup](#), described on [page 11-7](#)
 - [IP profile parameters](#), described on [page 11-23](#)

Easy Setup Profile configuration

The screen below is an example. Depending on the type of router you are using, fields displayed in this screen may vary.

Connection Profile 1: Easy Setup Profile

Address Translation Enabled:

Yes

IP Addressing...

Numbered

Local WAN IP Address:

206.1.1.6

Local WAN IP Mask:

255.255.255.0

Remote IP Address:

127.0.0.2

Remote IP Mask:

255.255.255.255

PPP Authentication...

PAP

Send User Name:

tonyf

Send Password:

PREVIOUS SCREEN

NEXT SCREEN

Return/Enter brings you to next screen.

The **Local WAN IP Address** is used to configure a NAT public address range consisting of the Local WAN IP Address and all its ports. The public address map list is named *Easy-PAT List* and the port map list is named *Easy-Servers*.

The two map lists, Easy-PAT List and Easy-Servers, are created by default and NAT configuration becomes effective. This will map all your private addresses (0.0.0.0 through 255.255.255.255) to your public address. These map lists are bound to the Easy Setup Profile. See [Binding Map Lists and Server Lists on page 11-23](#).

This is all you need to do if you want to continue to use a single PAT, or 1-to-many, NAT configuration.

Server Lists and Dynamic NAT configuration

You use the advanced NAT feature sets by first defining a series of mapping rules and then grouping them into a *list*. There are two kinds of lists – *map lists*, made up of dynamic, PAT and static mapping rules, and *server lists*, a list of internal services to be presented to the external world. Creating these lists is a four-step process:

1. **Define the public range** of addresses that external computers should use to get to the NAT internal machines. These are the addresses that someone on the Internet would see.
2. **Create a List name** that will act as a rule or server holder.
3. **Create a map or rule** that specifies the internal range of NATed addresses and the external range they are to be associated with.
4. **Associate the Map or Server List to your WAN interface** via a Connection Profile or the Default Profile.

The three NAT features all operate completely independently of each other, although they can be used simultaneously on the same Connection Profile.

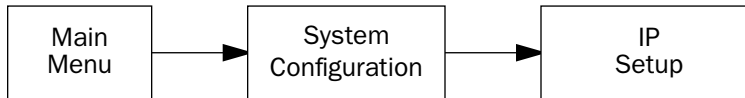
You can configure a simple 1-to-many PAT (often referred to simply as NAT) mapping using Easy Setup. More complex setups require configuration using the **Network Address Translation** item on the IP Setup screen.

An example MultiNAT configuration at the end of this chapter describes some applications for these features. See the [MultiNAT Configuration Example on page 11-29](#).

In order to configure the router to make servers on your LAN visible to the Internet, you use advanced features in the System Configuration screens, described in [IP setup](#).

IP setup

To access the NAT configuration screens, from the Main Menu navigate to IP Setup:



IP Setup

Ethernet IP Address:	192.168.1.1
Ethernet Subnet Mask:	255.255.255.0
Define Additional Subnets...	
Default IP Gateway:	127.0.0.2
Primary Domain Name Server:	0.0.0.0
Secondary Domain Name Server:	0.0.0.0
Domain Name:	isp.com
Receive RIP...	Both
Transmit RIP...	Off

Static Routes...
IP Address Serving...

Network Address Translation (NAT)...

Set up the basic IP attributes of your Netopia in this screen.

Select **Network Address Translation (NAT)** and press Return.

The Network Address Translation screen appears.

Network Address Translation

Add Public Range...
Show/Change Public Range...
Delete Public Range...

Add Map List...
Show/Change Map List...
Delete Map List...

Add Server List...
Show/Change Server List...
Delete Server List...

NAT Associations...

Return/Enter to configure IP Address redirection.

Public Range defines an external address range and indicates what type of mapping to apply when using this range. The types of mapping available are *dynamic*, *static* and *pat*.

Map Lists define collections of mapping rules. A rule maps interior range addresses to exterior range addresses by the mapping techniques defined in the map list.

Server Lists bind internal IP addresses and ports to external IP addresses and ports so that connections initiated from the outside can access an interior server.

NAT rules

The following rules apply to assigning NAT ranges and server lists:

- Static public address ranges must not overlap other static, PAT, public addresses, or the public address assigned to the router's WAN interface.
- A PAT public address must not overlap any static address ranges. It may be the same as another PAT address or server list address, but the port range must not overlap.

You configure the ranges of exterior addresses by first adding public ranges.

Select **Add Public Range** and press Return.

The Add NAT Public Range screen appears.

Add NAT Public Range

Range Name:	my_first_range
Type...	pat
Public Address:	206.1.1.6
First Public Port:	49152
Last Public Port:	65535
ADD NAT PUBLIC RANGE CANCEL	

- Select **Range Name** and give a descriptive name to this range.
- Select **Type** and from the pop-up menu, assign its type. Options are **static**, **dynamic**, or **pat** (the default).
 - If you choose pat as the range type, select **Public Address** and enter the exterior IP address in the range you want to assign. Select **First** and **Last Public Port** and enter the first and last exterior ports in the range. These are the ports that will be used for traffic initiated from the private LAN to the outside world.

Note: For PAT map lists and server lists, if you use the Public Address 0.0.0.0, the list will acquire its public IP address from the WAN IP address specified by your WAN IP configuration in the Connection Profile. If that is a static IP address, then the PAT map list and server lists will acquire that address. If it is a negotiated IP address, such as may be assigned via DHCP or PPP, the PAT map list and server lists will acquire that address each time it is negotiated.

- If you choose dynamic as the range type, a new menu item, **First Public Address**, becomes visible. Select **First Public Address** and enter the first exterior IP address in the range you want to assign. Select **Last Public Address** and enter an IP address at the end of the range.
- If you choose static as the range type, a new menu item, **First Public Address**, becomes visible. Select **First Public Address** and enter the first exterior IP address in the range you want to assign. Select **Last Public Address** and enter an IP address at the end of the range.
- Select **ADD NAT PUBLIC RANGE** and press Return. The range will be added to your list and you will be returned to the Network Address Translation screen.

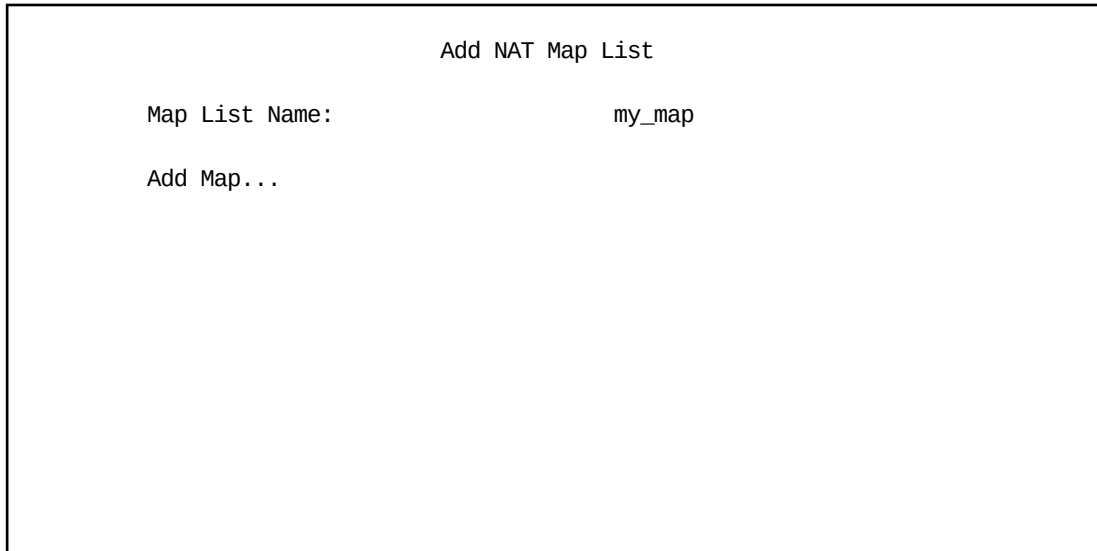
Note: We recommend that you use the pre-existing Easy PAT List which includes the default PAT rule and add your mappings to this.

11-10 Administration Guide

Once the public ranges have been assigned, the next step is to bind interior addresses to them. Because these bindings occur in ordered lists, called *map lists*, you must first define the list, then add mappings to it.

From the Network Address Translation screen select **Add Map List** and press Return.

The Add NAT Map List screen appears.

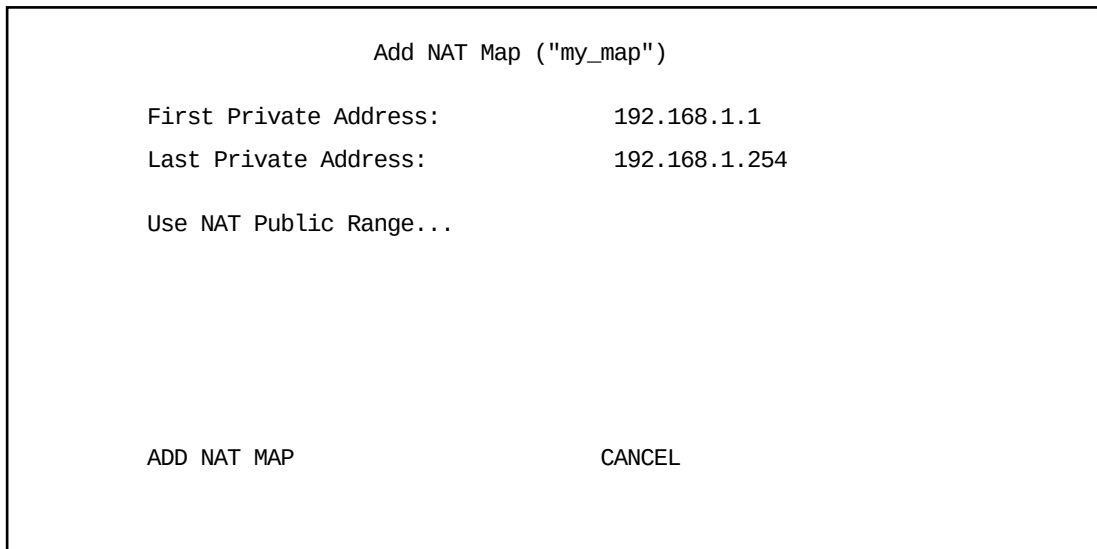


Add NAT Map List

Map List Name: my_map

Add Map...

- Select **Map List Name** and enter a descriptive name for this map list. A new menu item, **Add Map**, appears.
- Select **Add Map** and press Return. The Add NAT Map screen appears.



Add NAT Map ("my_map")

First Private Address: 192.168.1.1

Last Private Address: 192.168.1.254

Use NAT Public Range...

ADD NAT MAP CANCEL

- Select **First** and **Last Private Address** and enter the first and last interior IP addresses you want to assign

to this mapping.

- Select **Use NAT Public Range** and press Return. A screen appears displaying the public ranges you have defined.

Add NAT Map ("my_map")

+Public Address	Range	Type	Name
0.0.0.0	--	pat	Easy-PAT
206.1.1.6	--	pat	my_first_range
206.1.1.1	206.1.1.2	static	my_second_range
<<NEW RANGE...>>			

Select

Up/Down Arrow Keys to select, ESC to cancel, Return/Enter to Delete.

- From the list of public ranges you defined, select the one that you want to map to the interior range for this

mapping and press Return.

If none of your preconfigured ranges are suitable for this mapping, you can select **<<NEW RANGE>>** and create a new range. If you choose **<<NEW RANGE>>**, the Add NAT Public Range screen displays and you can create a new public range to be used by this map. See [Add NAT Public Range on page 11-9](#).

- The Add NAT Map screen now displays the range you have assigned.

Add NAT Map ("my_map")

First Private Address:	192.168.1.1
Last Private Address:	192.168.1.254
Use NAT Public Range...	my_first_range
Public Range Type is:	pat
Public Range Start Address is:	206.1.1.6

ADD NAT MAP

CANCEL

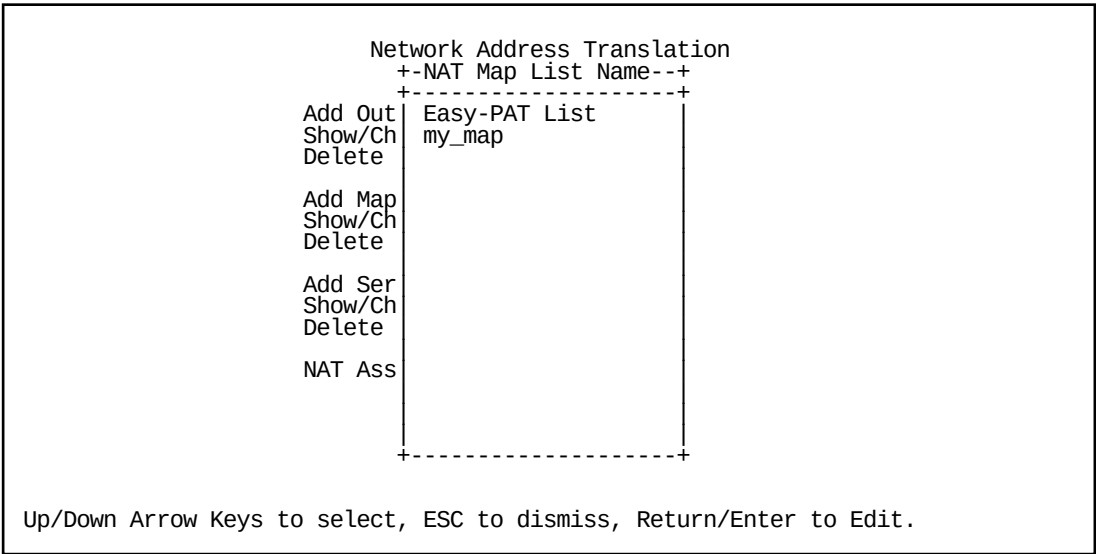
- Select **ADD NAT MAP** and press Return. Your mapping is added to your map list.

Modifying map lists

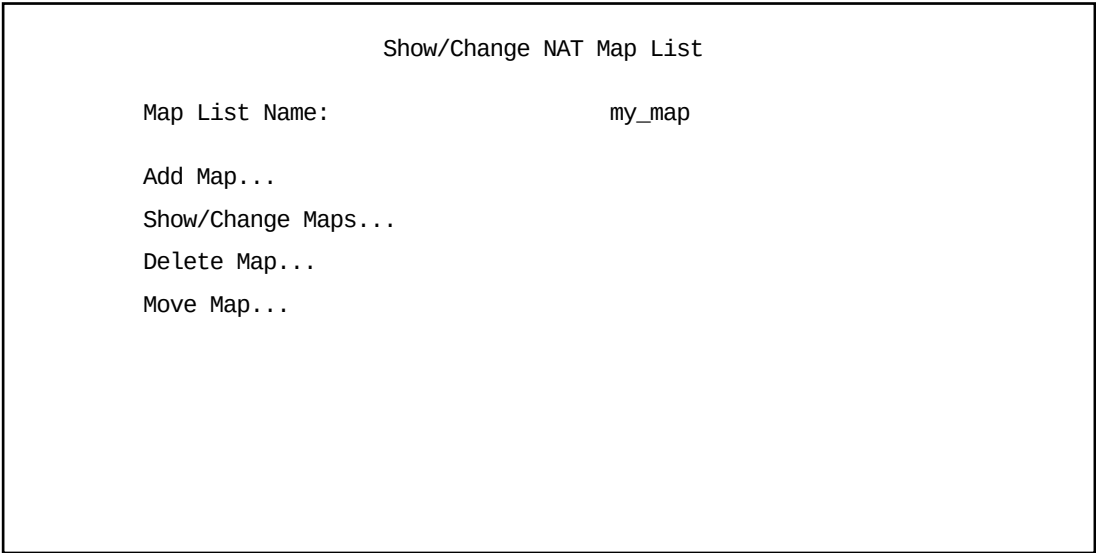
You can make changes to an existing map list after you have created it. Since there may be more than one map list you must select which one you are modifying.

From the Network Address Translation screen select **Show/Change Map List** and press Return.

- Select the map list you want to modify from the pop-up menu.



The Show/Change NAT Map List screen appears.



- **Add Map** allows you to add a new map to the map list.
- **Show/Change Maps** allows you to modify the individual maps within the list.
- **Delete Map** allows you to delete a map from the list.
- **Move Map** allows you to change the priority order in which the map is evaluated within the list. See [Moving maps on page 11-15](#).

Selecting **Show/Change Maps**, **Delete Map**, or **Move Map** displays the same pop-up menu.

Show/Change NAT Map List					
Private Address	Range	Type	Public Address	Range	
192.168.1.1	192.168.1.254	pat	206.1.1.6	--	
192.168.1.253	192.168.1.254	static	206.1.1.1	206.1.1.2	
192.168.1.1	192.168.1.252	dynamic	206.1.1.3	206.1.1.5	

Scroll to the map you want to modify using the arrow keys and press Return.

The Change NAT Map screen appears.

Change NAT Map ("my_map")

First Private Address:

192.168.1.253

Last Private Address:

192.168.1.254

Use NAT Public Range...

my_second_range

Public Range Type is:

static

Public Range Start Address is:

206.1.1.1

Public Range End Address is:

206.1.1.2

CHANGE NAT MAP

CANCEL

Make any modifications you need and then select **CHANGE NAT MAP** and press Return. Your changes will become effective and you will be returned to the Show/Change NAT Map List screen.

Moving maps

The Move Maps screen permits reordering the priority of maps in a map list. Since the maps are read from top to bottom, those at the top have the highest priority and those at the bottom have the lowest. If you used Easy Setup for your initial configuration, and added subsequent maps and server lists, you may need to reorder their priority since new maps are added to the top of the list.

Show/Change NAT Map List

Private Address Range	Type	Public Address Range
192.168.1.1	pat	206.1.1.6
192.168.1.252	static	206.1.1.1
192.168.1.2	dynamic	206.1.1.3

Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Edit.

In the example screen above, you may want to reorder the priority of the maps such that the dynamic map applies first and any additional traffic is routed via PAT or static.

All operations are done from a single pop-up menu.

- In the Show/Change Map List screen, select **Move Map**. A selection mode pop-up menu appears. In this mode you scroll to the map you want to move and press Return to select it for moving.
- After pressing **Return** you are in Move mode. Arrow keys move the selected map up or down. When you press Return again the map is put in the new location permanently and the pop-up menu is dismissed.

Show/Change NAT Map List

Private Address Range	Type	Public Address Range
192.168.1.2	dynamic	206.1.1.3
192.168.1.252	static	206.1.1.252
192.168.1.1	pat	206.1.1.1
192.168.1.251		206.1.1.2
		--

Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Edit.

- You can press Escape at any time in the pop-up menu to abort the move and restore the map list to its original ordering.

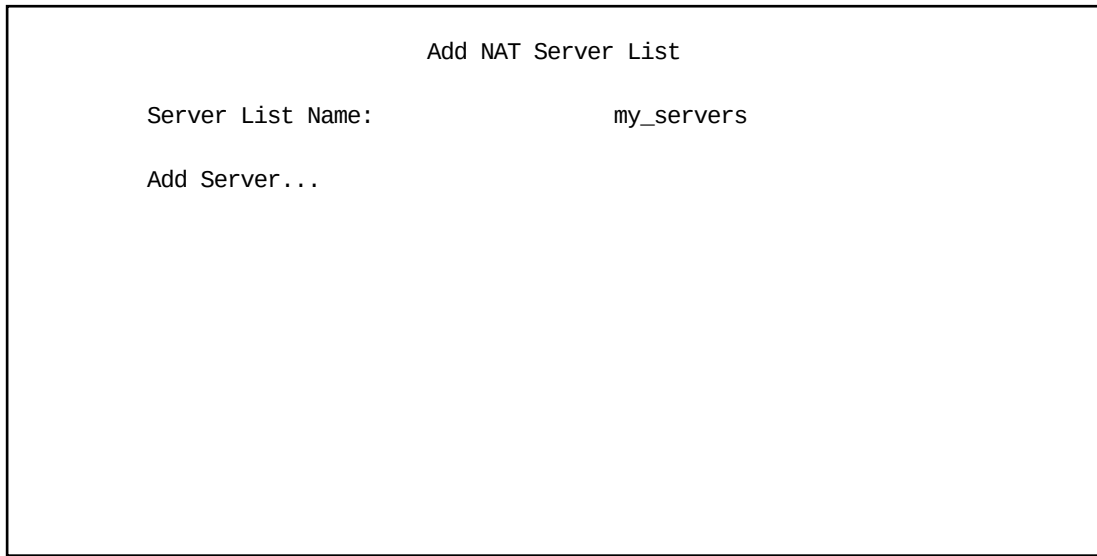
Note: The *pat* map is generally left at the bottom of the list.

Adding Server Lists

Server lists, also known as Exports, are handled similarly to map lists. If you want to make a particular server's port accessible (and it isn't accessible through other means, such as a static mapping), you must create a server list, or use the pre-existing Easy Servers list and add your entries to this list (preferred).

Select **Add Server List** from the Network Address Translation screen.

The Add NAT Server List screen appears.



Add NAT Server List

Server List Name: my_servers

Add Server...

- Select **Server List Name** and type in a descriptive name. A new menu item, **Add Server**, appears.

- Select **Add Server** and press Return. The Add NAT Server screen appears.

Add NAT Server ("my_servers")

Service...

Server Private IP Address: 192.168.1.45

Public IP Address: 206.1.1.1

ADD NAT SERVER
CANCEL

- Select **Service** and press Return. A pop-up menu appears listing a selection of commonly exported services.

Add NAT Server ("my_servers")

Service...

Server Private IP Address:

Public IP Address:

Type	Port(s)
ftp	21
telnet	23
smtp	25
tftp	69
gopher	70
finger	79
www-http	80
pop2	109
pop3	110
snmp	161 - 162
timbuktu	407
pptp	1723
irc	6665 - 6669
Other...	

ADD NAT SERVER
CANCEL

- Choose the service you want to export and press Return.

You can choose a preconfigured service from the list, or define your own by selecting **Other**. If you select **Other**, a screen is displayed that allows you to enter the port number range for your customized service.

Other Exported Port	
First Port Number (1..65535):	31337
Last Port Number (1..65535):	31337
OK CANCEL	

- Enter the **First** and **Last Port Number** between ports 1 and 65535. Select **OK** and press Return. You will be returned to the Add NAT Server screen.
- Enter the **Server Private IP Address** of the server whose service you are exporting.
 Since MultiNAT permits the mapping of multiple private IP addresses to multiple public IP addresses, your ISP or corporate site's router must be configured such that it knows that your multiple public addresses are accessible via your router.
 If you want to use static mappings to map internal servers to public addresses, your ISP or corporate site's router must also be configured for static routes to these public addresses on the Netopia Router.
- Enter the **Public IP Address** to which you are exporting the service.

Note: For PAT map lists and server lists, if you use the Public Address 0.0.0.0, the list will acquire its public IP address from the WAN IP address specified by your WAN IP configuration in the Connection Profile. If that is a static IP address, then the PAT map list and server lists will acquire that address. If it is a negotiated IP address, such as may be assigned via DHCP or PPP, the PAT map list and server lists will acquire that address each time it is negotiated.

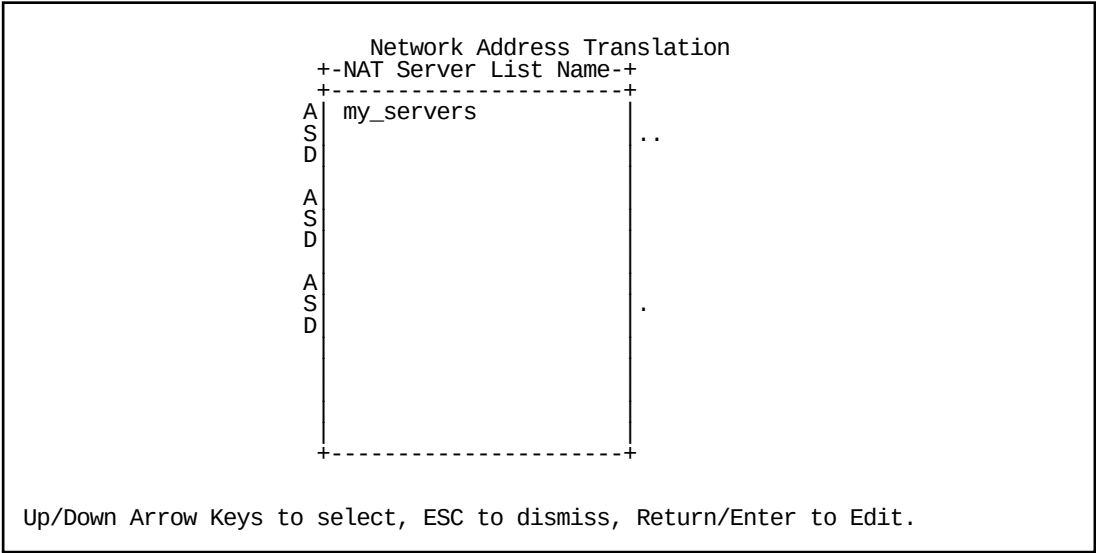
- Select **ADD NAT SERVER** and press Return. The server will be added to your server list and you will be returned to the Add NAT Server List screen.

Note: CUSeeMe (or other services that listen on specific ports) through MultiNat works as it did for non-MultiNat releases prior to version 4.4. In order to use **CUSeeMe** through the Netopia Router, you must export the ports 7648 and 7649. In MultiNat, you may use a port range export. Without the export, CUSeeMe will fail to work. This is true unless a static mapping is in place for the host using CUSeeMe. In that case no server list entry is necessary.

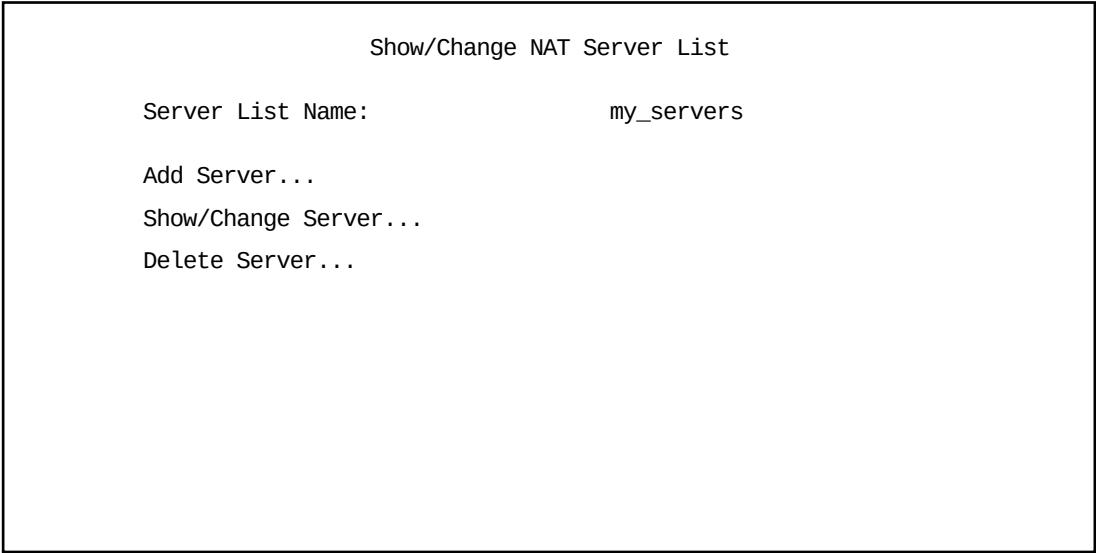
Modifying server lists

Once a server list exists, you can select it for modification or deletion.

- Select **Show/Change Server List** from the Network Address Translation screen.
- Select the Server List Name you want to modify from the pop-up menu and press Return.



The Show/Change NAT Server List screen appears.



- Selecting **Show/Change Server** or **Delete Server** displays the same pop-up menu.

Show/Change NAT Server List			
	+--Private Address--	Public Address--	Port-----+
Se	192.168.1.254	206.1.1.6	smtp
	192.168.1.254	206.1.1.5	smtp
	192.168.1.254	206.1.1.4	smtp
Ad	192.168.1.254	206.1.1.3	smtp
	192.168.1.254	206.1.1.1	smtp
Sh			
De			

Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Edit.

Select any server from the list and press Return. The Change NAT Server screen appears.

Change NAT Server ("My Exports")	
Service...	smtp
Server Private IP Address:	192.168.1.254
Public IP Address:	206.1.1.1
CHANGE NAT SERVER	CANCEL

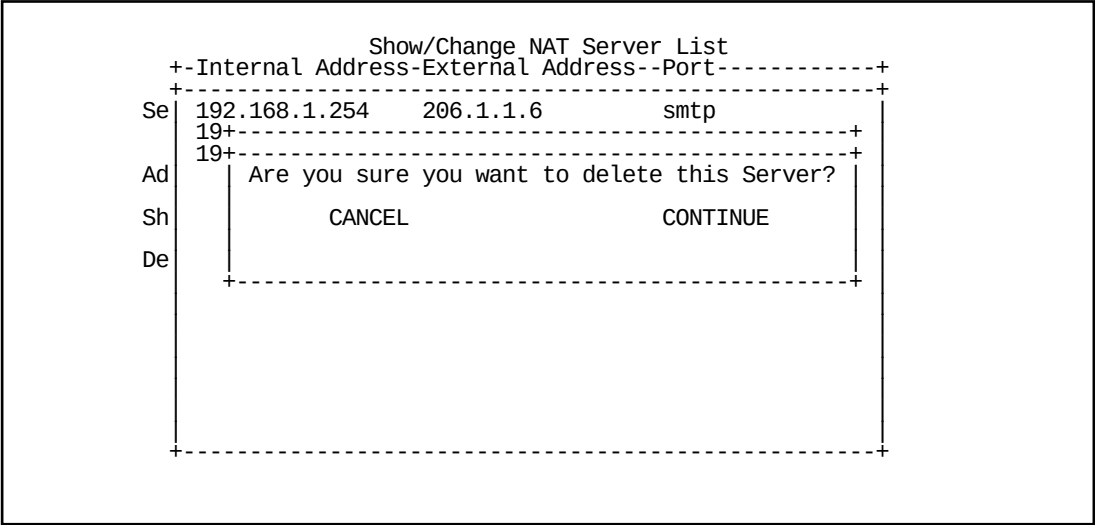
You can make changes to the server's service and port or internal or external address.

Select **CHANGE NAT SERVER** and press Return. Your changes take effect and you are returned to the Show/Change NAT Server List screen.

Deleting a server

To delete a server from the list, select **Delete Server** from the Show/Change NAT Server List menu and press Return.

A pop-up menu lists your configured servers. Select the one you want to delete and press Return. A dialog box asks you to confirm your choice.



Choose **CONTINUE** and press Return. The server is deleted from the list.

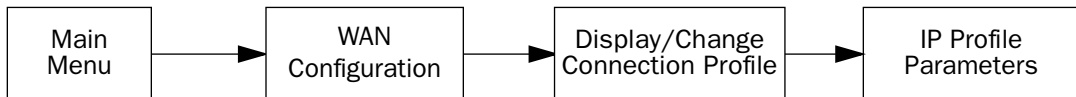
Binding Map Lists and Server Lists

Once you have created your map lists and server lists, for most Netopia Router models you must bind them to a profile, either a Connection Profile or the Default Profile. You do this in one of the following screens:

- the [IP profile parameters](#) screen (see below) of the Connection Profile configuration menu
- the [IP Parameters \(WAN Default Profile\)](#) screen (see [page 11-25](#)) of the Default Profile configuration menu
- the [Binding Map Lists and Server Lists](#) screen (see [page 11-23](#))

IP profile parameters

To bind a map list to a Connection Profile, from the Main Menu go to the WAN Configuration screen then the Display/Change Connection Profile screen. From the pop-up menu list of your Connection Profiles, choose the one you want to bind your map list to. Select **IP Profile Parameters** and press Return.



The IP Profile Parameters screen appears.

IP Profile Parameters	
Address Translation Enabled:	Yes
IP Addressing...	Unnumbered
NAT Map List...	Easy-PAT List
NAT Server List...	Easy-Servers
Local WAN IP Address:	206.1.1.6
Remote IP Address:	127.0.0.2
Remote IP Mask:	255.255.255.255
Filter Set...	Basic Firewall
Remove Filter Set	
RIP Profile Options... Configure IP requirements for a remote network connection here.	

- Select **NAT Map List** and press Return. A pop-up menu displays a list of your defined map lists.

IP Profile Parameters

+--NAT Map List Name--+

Address Trans

IP Addressing

NAT Map List.

NAT Server Li

Local WAN IP

Remote IP Add

Remote IP Mas

Filter Set...

Remove Filter

Receive RIP:

Easy-PAT

my_map

<<None>>

s

mbered

sy PAT

7.0.0.2

5.255.255.255

tBIOS Filter

th

Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Edit.

- Select the map list you want to bind to this Connection Profile and press Return. The map list you selected will now be bound to this Connection Profile.
- Select **NAT Server List** and press Return. A pop-up menu displays a list of your defined server lists.

IP Profile Parameters

+--NAT Server List Name--+

Address Trans

IP Addressing

NAT Map List.

NAT Server Li

Local WAN IP

Local WAN IP

Remote IP Add

Remote IP Mas

Filter Set...

Remove Filter

Receive RIP:

Easy-Servers

my_servers

<<None>>

s

mbered

sy PAT

0.0.0

0.0.0

7.0.0.2

5.255.255.255

tBIOS Filter

th

Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Edit.

- Select the server list you want to bind to this Connection Profile and press Return. The server list you selected will now be bound to this Connection Profile.

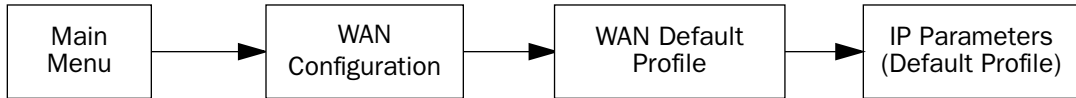
Note: There is no interdependency between NAT and IP Addressing. Also, the Local WAN IP Address and Mask fields' visibility are dependent only on the IP Addressing type.

IP Parameters (WAN Default Profile)

The Netopia 4753 in HDLC (Copper Mountain) Operation Mode supports a WAN default profile that permits several parameters to be configured without an explicitly configured Connection Profile.

The procedure is similar to the procedure to bind map lists and server lists to a Connection Profile.

From the Main Menu go to the WAN Configuration screen, then the Default Profile screen. Select **IP Parameters** and press Return.



The IP Parameters (Default Profile) screen appears.

IP Parameters (Default Profile)

Address Translation Enabled:	Yes
NAT Map List...	Easy-PAT List
NAT Server List...	Easy-Servers
Filter Set (Firewall)...	
Remove Filter Set	
Receive RIP:	Both

Return/Enter to select <among/between> ...

- Toggle **Address Translation Enabled** to Yes.

- Select **NAT Map List** and press Return. A pop-up menu displays a list of your defined map lists.

IP Parameters (Default Profile)
+--NAT Map List Name--+
+-----+
Easy-PAT List
my_map
<<None>>
s

Address Trans
NAT Map List.
NAT Server Li
Filter Set (F
Remove Filter
Receive RIP:
th

Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Edit.

- Select the map list you want to bind to the default profile and press Return. The map list you selected will now be bound to the default profile.
- Select **NAT Server List** and press Return. A pop-up menu displays a list of your defined server lists.

IP Parameters (Default Profile)
+--NAT Server List Name--+
+-----+
Easy-Servers
my_servers
<<None>>
s

Address Trans
NAT Map List.
NAT Server Li
Filter Set (F
Remove Filter
Receive RIP:
th

Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Edit.

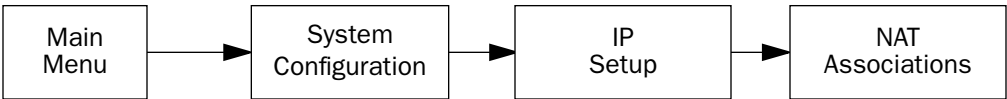
- Select the server list you want to bind to the default profile and press Return. The server list you selected will now be bound to the default profile.

Note: There is no interdependency between NAT and IP Addressing. Also, the Local WAN IP Address and Mask fields' visibility are dependent only on the IP Addressing type.

NAT Associations

Configuration of map and server lists alone is not sufficient to enable NAT for a WAN connection because map and server lists must be linked to a profile that controls the WAN interface. This can be a Connection Profile, a WAN Ethernet interface, a default profile, or a default answer profile. Once you have configured your map and server lists, you may want to reassign them to different interface-controlling profiles, for example, Connection Profiles. To permit easy access to this IP Setup functionality, you can use the NAT Associations screen.

You access the NAT Associations screen from the Network Address Translation screen.



Select **NAT Associations** and press Return. The NAT Associations screen appears.

NAT Associations			
Profile/Interface Name-----	Nat?	Map List Name-----	Server List Name
Default Answer Profile	On	my_first_map	my_servers
Easy Setup Profile	On	Easy-PAT	my_servers
Profile 01	On	my_second_map	my_servers
Profile 02	On	my_first_map	my_server_list
Profile 03	On	<<None>>	<<None>>

- You can toggle **NAT? On** or **Off** for each Profile/Interface name. You do this by navigating to the **NAT?** field associated with each profile using the arrow keys. Toggle NAT on or off by using the Tab key.
- You can reassign any of your map lists or server lists to any of the Profile/Interfaces. You do this by navigating to the **Map List Name** or **Server List Name** field associated with each profile using the arrow

keys. Select the item by pressing Return to display a pop-up menu of all of your configured lists.

NAT Associations

+NAT Map List Name+

Profile/Interface Name-----	Nat+		Server List Name
Easy Setup Profile	On	Easy-PAT List	my_servers
Profile 01	On	my_first_map	my_servers
Profile 02	On	my_second_map	my_server_list
Profile 03	On	my_map	<<None>>
Profile 04	On	<<None>>	<<None>>

Default Answer Profile

On

+-----+my_servers

Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Edit.

- Select the list name you want to assign and press Return again. Your selection will then be associated with the corresponding profile or interface.

MultiNAT Configuration Example

To help you understand a typical MultiNAT configuration, this section describes an example of the type of configuration you may want to implement on your site. The values shown are for example purposes only. *Make your own appropriate substitutions.*

A typical DSL service from an ISP might include five user addresses. Without PAT, you might be able to attach only five IP hosts. Using simple 1-to-many PAT you can connect more than five devices, but use only one of your addresses. Using multiNAT you can make full use of the address range. The example assumes the following range of addresses offered by a typical ISP:

Local WAN IP address:	206.1.1.6
Local WAN subnet mask:	255.255.255.248
Remote IP address:	206.1.1.254
Default gateway:	206.1.1.254

Public IP addresses assigned by the ISP are 206.1.1.1 through 206.1.1.6 (255.255.255.248 subnet mask).

Your internal devices have IP addresses of 192.168.1.1 through 192.168.1.254 (255.255.255.0 subnet mask).

Netopia Router's Ethernet address is:	192.168.1.1
Web server's address is:	192.168.1.253
Mail server's address is:	192.168.1.254
FTP server's address is:	192.168.1.253

In this example you will statically map the first five public IP addresses (206.1.1.1 - 206.1.1.5) to the first five corresponding private IP addresses (192.168.1.1 - 192.168.1.5). You will use these 1-to-1 mapped addresses to give your servers “real” addresses. You will then map 206.1.1.6 to the remaining private IP addresses (192.168.1.6 - 192.168.1.254) using PAT.

The configuration process is as follows:

From the Main Menu go to the Easy Setup and then the Connection Profile screen.



Enter your ISP-supplied values as shown below.

Connection Profile 1: Easy Setup Profile

Connection Profile Name:

Easy Setup Profile

Address Translation Enabled:

Yes

IP Addressing...

Numbered

Local WAN IP Address:

206.1.1.6

Local WAN IP Mask:

255.255.255.248

PREVIOUS SCREEN

NEXT SCREEN

Enter a subnet mask in decimal and dot form (xxx.xxx.xxx.xxx).

Enter basic information about your WAN connection with this screen.

Select **NEXT SCREEN** and press Return.

Your IP values are shown here.

IP Easy Setup

Ethernet IP Address:

192.168.1.1

Ethernet Subnet Mask:

255.255.255.0

Domain Name:

ISP.net

Primary Domain Name Server:

173.166.101.1

Secondary Domain Name Server:

173.166.102.1

Default IP Gateway:

206.1.1.254

IP Address Serving:

On

Number of Client IP Addresses:

20

1st Client Address:

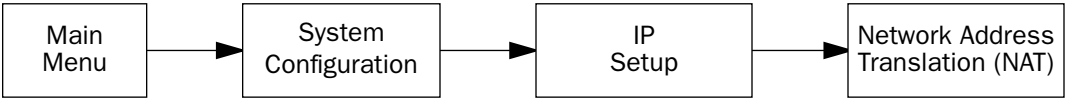
192.168.1.2

PREVIOUS SCREEN

NEXT SCREEN

Set up the basic IP & IPX attributes of your Netopia in this screen.

Then navigate to the Network Address Translation (NAT) screen.



Select **Show/Change Public Range**, then **Easy-PAT Range**, and press Return. Enter the value your ISP assigned for your public address (206.1.1.6, in this example). Toggle **Type** to pat. Your public address is then mapped to the remaining private IP addresses using PAT. (If you were not using the Easy-PAT Range and Easy-PAT List that are created by default by using Easy Setup, you would have to *define* a public range and map list. For the purpose of this example you can just *alter* this range and list.)

Change NAT Public Range	
Range Name:	Easy-PAT Range
Type...	pat
Public Address:	206.1.1.6
First Public Port:	49152
Last Public Port:	65535
CHANGE NAT PUBLIC RANGE	CANCEL

Select **CHANGE NAT PUBLIC RANGE** and press Return. This returns you to the Network Address Translation screen.

Select **Add Public Range** and press Return. Type a name for this static range, as shown below. Enter the first and last public addresses your ISP assigned in their respective fields as shown. The first five public IP addresses (206.1.1.1 - 206.1.1.5, in this example) are statically mapped to the first five corresponding private IP addresses (192.168.1.1 - 192.168.1.5).

Add NAT Public Range	
Range Name:	Static Range
Type...	static
First Public Address:	206.1.1.1
Last Public Address:	206.1.1.5
ADD NAT PUBLIC RANGE	CANCEL

Return/Enter to commit changes.

Select **ADD NAT PUBLIC RANGE** and press Return. You are returned to the Network Address Translation screen.

Next, select **Show/Change Map List** and choose **Easy-PAT List**. Select **Add Map**. The **Add NAT Map** screen appears. (Now the name *Easy-PAT List* is a misnomer since it has a static map included in its list.) Enter in 192.168.1.1 for the **First Private Address** and 192.168.1.5 for the **Last Private Address**.

Add NAT Map ("Easy-PAT List")

First Private Address:

192.168.1.1

Last Private Address:

192.168.1.5

Use NAT Public Range...

ADD NAT MAP

CANCEL

Select **Use NAT Public Range** and from the pop-up menu choose **Static Range**. Select **ADD NAT MAP** and press Return.

Navigate to the Show/Change NAT Map List screen (see [Moving maps on page 11-15](#)) to move the static map above the default PAT rule in the Map List.

This will statically map the first five public IP addresses to the first five corresponding private IP addresses and will map 206.1.1.6 to the remaining private IP addresses using PAT.

Notes on the example

The Easy-Map List and the Easy-PAT List are attached to any new Connection Profile by default. If you want to use this NAT configuration on a previously defined Connection Profile then you need to *bind* the Map List to the profile. You do this through either the NAT Associations screen or the profile's configuration screens.

The PAT part of this example setup will allow any user on the Netopia Router's LAN with an IP address in the range of 192.168.1.6 through 192.168.1.254 to *initiate* traffic flow to the outside world (for example, the Internet). No one on the Internet would be able to initiate a conversation with them.

The Static mapping part of this example will allow any of the machines in the range of addresses from 192.168.1.1 through 192.168.1.5 to communicate with the outside world as if they were at the addresses 206.1.1.1 through 206.1.1.5, respectively. It also allows any machine on the Internet to access any service (port) on any of these five machines.

You may decide this poses a security risk. You may decide that anyone can have complete access to your FTP server, but not to your router, and only limited access to the desired services (ports) on the Web and Mail servers.

To make these changes, first limit the range of remapped addresses on the Static Map and then edit the default server list called Easy-Servers.

- First, navigate to the **Show/Change Map List** screen, select **Easy-PAT List** and then **Show/Change Maps**. Choose the **Static Map** you created and change the **First Private Address** from 192.168.1.1 to 192.168.1.4. Now the router, Web, and Mail servers' IP addresses are no longer included in the range of static mappings and are therefore no longer accessible to the outside world. Users on the Internet will not be able to Telnet, Web, SNMP, or ping to them. It is best also to navigate to the public range screen and change the **Static Range** to go from 206.1.1.5.
- Next, navigate to **Show/Change Server List** and select **Easy-Servers** and then **Add Server**. You should export both the Web (www-http) and Mail (smtp) ports to one of the now free public addresses. Select **Service...** and from the resulting pop-up menu select **www-http**. In the resulting screen enter your Web server's address, 192.168.1.2, and the public address, for example, 206.1.1.2, and then select **ADD NAT SERVER**. Now return to **Add Server**, choose the **smtp** port and enter 192.168.1.3, your Mail server's IP address for the **Server Private IP Address**. You can decide if you want to present both your Web and Mail services as being on the same public address, 206.1.1.2, or if you prefer to have your Mail server appear to be at a different IP address, 206.1.1.3. For the sake of this example, alias both services to 206.1.1.2.

Now, as before, the PAT configuration will allow any user on the Netopia Router's LAN with an IP address in the range of 192.168.1.6 through 192.168.1.254 to initiate traffic flow to the Internet. Someone at the FTP server can access the Internet and the Internet can access all services of the FTP machine as if it were at 206.1.1.5. The server cannot directly communicate with the outside world. The only communication between the Web server and the Internet is through port 80, the Web port, as if the server were located on a machine at IP address 206.1.1.2. Similarly, the only communication with the Mail server is through port 25, the SMTP port, as if it were located at IP address 206.1.1.2.

Chapter 12

Virtual Private Networks (VPNs)

The Netopia 4753 offers IPsec, PPTP, and ATMP tunneling support for Virtual Private Networks (VPN).

The following topics are covered in this chapter:

- [Overview on page 12-1](#)
- [About PPTP Tunnels on page 12-3](#)
- [About IPsec Tunnels on page 12-7](#)
- [Encryption Support on page 12-12](#)
- [ATMP/PPTP Default Answer Profile on page 12-13](#)
- [VPN QuickView on page 12-14](#)
- [Dial-Up Networking for VPN on page 12-15](#)
- [About ATMP Tunnels on page 12-19](#)
- [Allowing VPNs through a Firewall on page 12-21](#)

Overview

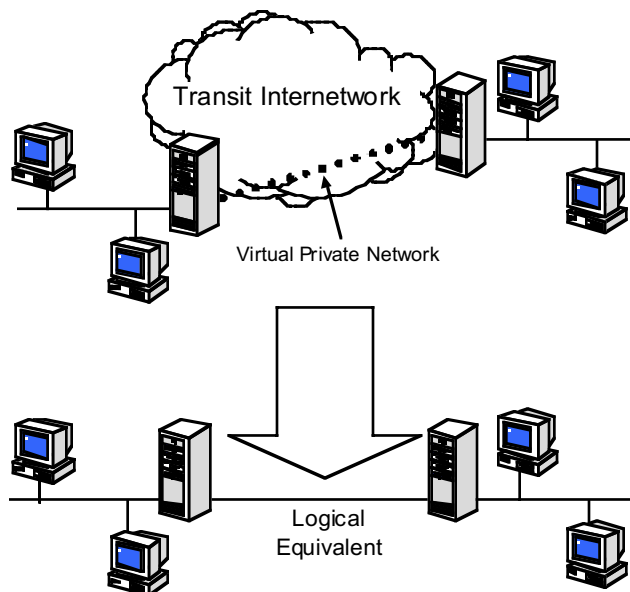
When you make a long distance telephone call from your home to a relative far away, you are creating a private network. You can hold a conversation, and exchange information about the happenings on opposite sides of the state, or the continent, that you are mutually interested in. When your next door neighbor picks up the phone to call her daughter at college, at the same time you are talking to your relatives, your calls don't overlap, but each is separate and private. Neither house has a direct wire to the places they call. Both share the same lines on the telephone poles (or underground) on the street.

These calls are *virtual private networks*. *Virtual*, because they appear to be direct connections between the calling and answering parties, even though they travel over the public wires and switches of the phone company; *private*, because neither pair of calling and answering parties interacts with the other; and *networks*, because they exchange information.

Computers can do the same thing; it's called Virtual Private Networks (VPNs). Equipped with a Netopia 4753, a single computer or private network (LAN) can establish a private connection with another computer or private network over the public network (Internet).

The Netopia 4753 can be used in VPNs either to initiate the connection or to answer it. When used in this way, the routers are said to be *tunnelling* through the public network (Internet). The advantages are that, like your long distance phone call, you don't need a direct line between one computer or LAN and the other, but use the local connections, making it much cheaper; and the information you exchange through your tunnel is private and secure.

Tunneling is a process of creating a private path between a remote user or private network and another private network over some intermediate network, such as the IP-based Internet. A VPN allows remote offices or employees access to your internal business LAN through means of encryption allowing the use of the public Internet to look “virtually” like a private secure network. When two networks communicate with each other through a network based on the Internet Protocol, they are said to be *tunneling* through the IP network.



Unlike the phone company, private and public computer networks can use more than one protocol to carry your information over the wires. Three such protocols are in common use for tunnelling: Point-to-Point Tunnelling Protocol (PPTP), Ascend Tunnel Management Protocol (ATMP), and IP Security (IPsec). The Netopia Router can use any one.

- Point-to-Point Tunneling Protocol (PPTP) is an extension of Point-to-Point Protocol (PPP) and uses a client and server model. Netopia’s PPTP implementation is compatible with Microsoft’s and can function as either the client (PAC) or the server (PNS). As a client, a Netopia R-series router can provide all users on a LAN with secure access over the Internet to the resources of another LAN by setting up a tunnel with a Windows NT server running Remote Access Services (RAS) or with another Netopia Router. As a server, a Netopia R-series router can provide remote users a secure connection to the resources of the LAN over a dial-up, cable, DSL, or any other type of Internet access. Because PPTP can create a VPN tunnel using the Dial-Up Networking (DUN) (see [Dial-Up Networking for VPN on page 12-15](#)) utility built into Windows 95, 98, or NT, no additional client software is required.
- Ascend Tunnel Management Protocol (ATMP) is the protocol that is implemented in many Ascend routers. ATMP is a simple protocol for connecting nodes and/or networks together over the Internet via a tunnel. ATMP encapsulates IP or other user data without PPP headers within General Routing Encapsulation (GRE) protocol over IP. ATMP is more efficient than PPTP for network-to-network tunnels.

When used to initiate the tunnelled connection, the Netopia 4753 is called a *PPTP Access Concentrator* (PAC, in PPTP language), or a *foreign agent* (in ATMP language). When used to answer the tunnelled connection, the Netopia Router is called a *PPTP Network Server* (PNS, in PPTP language) or a *home agent* (in ATMP language).

In either case, the Netopia Router wraps, or encapsulates, information that one end of the tunnel exchanges with the other, in a wrapper called General Routing Encapsulation (GRE), at one end of the tunnel, and unwraps, or decapsulates, it at the other end.

- *IPsec* stands for IP Security, a set of protocols that supports secure exchange of IP packets at the IP layer. IPsec is deployed widely to implement Virtual Private Networks (VPNs). IPsec supports two encryption modes: Transport and Tunnel. Transport mode encrypts only the data portion (payload) of each packet, but leaves the header untouched. The more secure Tunnel mode encrypts both the header and the payload. On the receiving side, an IPsec-compliant device decrypts each packet. The Netopia 4753 supports the more secure Tunnel mode.

DES stands for Data Encryption Standard, a popular symmetric-key encryption method. DES uses a 56-bit key. The Netopia 4753 offers IPsec DES encryption over the VPN tunnel.

Configuring the Netopia Router for use with the different protocols is done through the console-based menu screens. Each type is described in its own section:

- [About PPTP Tunnels on page 12-3](#)
- [About IPsec Tunnels on page 12-7](#)
- [About ATMP Tunnels on page 12-19](#)

Your configuration depends on which protocol you (and the router at the other end of your tunnel) will use, and whether or not you will be using the VPN client software in a standalone remote connection.

Having both an ATMP tunnel and a PPTP export is not possible because functions require GRE and the router's PPTP export/server does not distinguish the GRE packets it forwards. Since it processes all of them, ATMP tunneling is impaired. For example, you cannot run an ATMP tunnel between two routers and also have PPTP exported on one side.

Summary

A Virtual Private Network (VPN) connects the components of one network over another network. VPNs accomplish this by allowing you to *tunnel* through the Internet or another public network in a manner that provides the same security and features formerly available only in private networks.

VPNs allow networks to communicate across an IP network. Your local networks (connected to the Netopia Router) can exchange data with remote networks that are also connected to a VPN-capable router.

This feature provides individuals at home, on the road, or in branch offices with a cost-effective and secure way to access resources on remote LANs connected to the Internet with Netopia Routers. The feature is built around three key technologies: PPTP, IPsec, and ATMP.

About PPTP Tunnels

To set up a PPTP tunnel, you create a Connection Profile including the IP address and other relevant information for the remote PPTP partner. You use the same procedure to initiate a PPTP tunnel that terminates at a remote PPTP server or to terminate a tunnel initiated by a remote PPTP client.

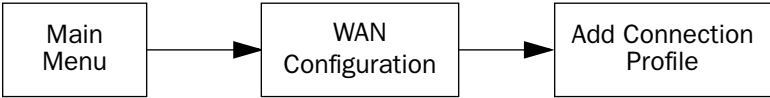
PPTP configuration

To set up the router as a PPTP Network Server (PNS) capable of answering PPTP tunnel requests you must also configure the VPN Default Answer Profile. See [ATMP/PPTP Default Answer Profile on page 12-13](#) for more information.

PPTP is a Datalink Encapsulation option in Connection Profiles. It is not an option in device or link configuration screens, as PPTP is not a native encapsulation. Consequently, the Easy Setup Profile does not offer PPTP datalink encapsulation. See the *User's Reference Guide* for information on creating Connection Profiles.

Channel 4 (and higher) events, such as connections and disconnections, reported in the WAN Event Histories are VPN tunnel events.

To define a PPTP tunnel, navigate to the Add Connection Profile menu from the Main Menu.



Add Connection Profile

Profile Name:

Profile Enabled:

Data Link Encapsulation...

IP Profile Parameters...

Profile 1

+-----+

+-----+

PPP

Frame Relay

RFC1483

ATMP

PPTP

IPsec

+-----+

COMMIT

CANCEL

When you define a Connection Profile as using PPTP by selecting PPTP as the datalink encapsulation method, and then select **Data Link Options**, the PPTP Tunnel Options screen appears.

PPTP Tunnel Options	
PPTP Partner IP Address:	173.167.8.134
Tunnel Via Gateway:	0.0.0.0
Data Compression...	None
Authentication...	CHAP
Send Host name:	tony
Send Secret:	*****
Receive Host name:	kimba
Receive Secret:	*****
Initiate Connections:	Yes
On Demand:	Yes
Optional Windows NT Domain Name:	
Idle Timeout (seconds):	300

Return accepts * ESC cancels * Left/Right moves insertion point * Del deletes.
In this Screen you will configure the GRE/PPTP specific connection params.

Note: Profiles using PPTP do not offer a Telco Options screen.

- Enter the **PPTP Partner IP Address**. This specifies the address of the other end of the tunnel.

If you do not specify the PPTP Partner IP Address the gateway cannot initiate tunnels, i.e., act as a PPTP Access Concentrator (PAC) for this profile. It can only accept tunnel requests as a PPTP Network Server (PNS).

- If you specify the PPTP Partner IP Address, and the address is in the same subnet as the Remote IP Address you specified in the IP Profile Parameters, the **Tunnel Via Gateway** option becomes visible. You can enter the address by which the gateway partner is reached.

If you do not specify the PPTP Partner IP Address, the router will use the default gateway to reach the partner and the **Tunnel Via Gateway** field is hidden. If the partner should be reached via an alternate port (i.e. the LAN instead of the WAN), the **Tunnel Via Gateway** field allows this path to be resolved.

- You can specify a **Data Compression** algorithm, either None or Standard LZS, for the PPTP connection.

Note: When the Authentication protocol is MS-CHAP, compression is set to None, and the **Data Compression** option is hidden.

- From the pop-up menu select an **Authentication** protocol for the PPP connection. Options are PAP, CHAP, or MS-CHAP. The default is PAP. The authentication protocol must be the same on both ends of the tunnel.
- When the authentication protocol is MS-CHAP, you can specify a **Data Encryption** algorithm for the PPTP connection. Available options are MPPE and None (the default). For other authentication protocols, this option is hidden. When MPPE is negotiated, the WAN Event History reports that it is negotiated as a CCP (compression) type. This is because the MPPE protocol uses a compression engine, even though it is not

itself a compression protocol.

Note: The Netopia 4753 supports 128-bit (“strong”) encryption. Unlike MS-CHAP version 1, which supports one-way authentication, MS-CHAP version 2 supports mutual authentication between connected routers and is incompatible with MS-CHAP version 1 (MS-CHAP-V1). When you choose MS-CHAP as the authentication method for the PPTP tunnel, the Netopia router will start negotiating MS-CHAP-V2. If the router you are connecting to does not support MS-CHAP-V2, it will fall back to MS-CHAP-V1, or, if the router you are connecting to does not support MPPE at all, the PPP session will be dropped.

- You can specify a **Send Host Name** which is used with Send Secret for authenticating with a remote PNS when the profile is used for initiating a tunnel connection.
- You must specify a **Send Secret** (the CHAP and MS-CHAP term for password), used for authenticating the tunnel when initiating a tunnel connection.
- You can specify a **Receive Host Name** which is used with the Receive Secret for authenticating a remote PPTP client.
- You must specify a **Receive Secret**, used for authenticating the remote PPTP client.
- You can specify that this router will **Initiate Connections** (acting as a PAC) or only answer them (acting as a PNS).
- Tunnels are normally initiated **On Demand**; however, you can disable this feature. When disabled, the tunnel must be manually established via the call management screens or may be scheduled using the scheduled connections feature. See “Scheduled Connections” in the *User’s Reference Guide*.
- Some networks that use Microsoft Windows NT PPTP Network Servers require additional authentication information, called *Windows NT Domain Name*, when answering PPTP tunnel connection requests. Not all Windows NT installations require this information, since not all such installations use this authentication feature. The Windows NT Domain Name is not the same as the Internet domain name, but is the name of a group of servers that share common security policy and user account databases. Your PPTP tunnel partner’s administrator will supply this Windows NT Domain Name if it is required. If you configure your Netopia 4753 to initiate PPTP tunnel connections by toggling **Initiate Connections** to **Yes**, the **Optional Windows NT Domain Name** field appears. Enter the domain name your network administrator has supplied.
- You can specify the **Idle Timeout**, an inactivity timer, whose expiration will terminate the tunnel. A value of zero disables the timer. Because tunnels are subject to abrupt termination when the underlying datalink is torn down, use of the Idle Timeout is strongly encouraged.
- Return to the Connection Profile screen by pressing Escape.
- Select **IP Profile Parameters** and press Return.

The IP Profile Parameters screen appears.

IP Profile Parameters

Address Translation Enabled:	Yes
NAT Map List...	Easy-PAT
NAT Server List...	Easy-Servers
Local WAN IP Address:	0.0.0.0
Remote IP Address:	173.167.8.10
Remote IP Mask:	255.255.0.0
Filter Set...	
Remove Filter Set	
Receive RIP:	Both

Enter a subnet mask in decimal and dot form (xxx.xxx.xxx.xxx).

- Enter the **Remote IP Address** and **Remote IP Mask** for the host to which you want to tunnel. The remote IP address and remote IP mask refer to the remote private network into which your device will be tunnelling.

About IPsec Tunnels

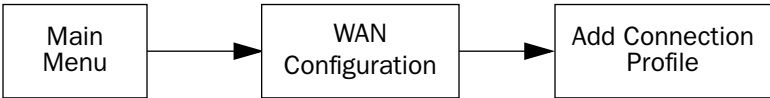
IPsec stands for IP Security, a set of protocols that supports secure exchange of IP packets at the IP layer. IPsec is deployed widely to implement Virtual Private Networks (VPNs). See [Overview on page 12-1](#) for more information.

IPsec supports two encryption modes: Transport and Tunnel. Transport mode encrypts only the data portion (payload) of each packet, but leaves the header untouched. The more secure Tunnel mode encrypts both the header and the payload. On the receiving side, an IPsec-compliant device decrypts each packet. Netopia Routers support the more secure Tunnel mode.

DES stands for Data Encryption Standard, a popular symmetric-key encryption method. DES uses a 56-bit key. The Netopia 4753 offers IPsec DES encryption over the VPN tunnel.

Configuration

IPsec tunnels are defined in the same manner as PPTP tunnels. You configure the Connection Profile as follows. From the Main Menu navigate to WAN Configuration and then Add Connection Profile.



The Add Connection Profile screen appears.

Add Connection Profile

Profile Name:
Profile Enabled:

Profile 1
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+

Data Link Encapsulation...
Data Link Options...

PPP
Frame Relay
RFC1483
ATMP
PPTP
IPsec

IP Profile Parameters...

COMMIT

CANCEL

- From the **Data Link Encapsulation** pop-up menu select **IPsec**.
- Then select **Data Link Options**. The IPsec Encryption & Authentication Options screen appears.

IPsec Encryption & Authentication Options

Encryption Transform...
Encryption Key:

+-----+
+-----+
+-----+
+-----+

Authentication Type...
Authentication Transform...
Authentication Key:

ESP
HMAC-MD5-96

COMMIT

CANCEL

- You must specify an **Encryption Transform**. The choices are **DES** or **NULL**. The default is **DES**.

IPsec Encryption & Authentication Options	
Encryption Transform...	DES
Encryption Key:	
Authentication Type...	ESP
Authentication Transform...	HMAC-MD5-96
Authentication Key:	
COMMIT	CANCEL
Enter a key of 16 Hex digits, e.g. '1234567890ABCDEF'	

- You must enter an **Encryption Key** if the Encryption Transform is DES. The key for DES must be a hexadecimal string of 16 characters, using Hex characters only: '0'-'9', 'A'-'F' and 'a' - 'f'. No key entry appears if the encryption transform is NULL.
 - You must specify an **Authentication Type**. The default is **ESP**, and the choices are **ESP**, **None**, or **AH**. **ESP** provides confidentiality over the IP payload and optional authentication of the IP payload and ESP header. **AH** (Authentication Header) provides authentication over the immutable parts of the IP header, AH header and the IP payload. ESP is preferred.
 - You must specify an **Authentication Transform** if the Authentication Type is anything other than None. The default is **HMAC-MD5-96**, and the choices are **HMAC-MD5-96** or **HMAC-SHA1-96** for both AH and ESP.
 - You must specify an **Authentication Key** if the Authentication Type is anything other than None. The key must be an ASCII string of up to 48 characters for both HMAC-MD5-96 and HMAC-SHA1-96.
- Key:** The key is a hexadecimal entry of 16 bytes (32 characters of input) for MD5 and 20 bytes (40 characters of input) for SHA1. It is not possible to view the Encryption Keys or Authentication Key once they have been set.
- Press **COMMIT** to return to the Add Connection Profile screen.
 - Select **IP Profile Parameters**.

IP Profile Parameters

The following IP Profile Options screen is displayed for an IPsec Connection Profile.

IP Profile Options	
SPI (Security Parameters Index):	123456789
Remote Tunnel Endpoint Address:	0.0.0.0
Remote Members Network:	0.0.0.0
Remote Members Mask:	0.0.0.0
Address Translation Enabled:	Yes
NAT Map List...	Easy-PAT List
NAT Server List...	Easy-Servers
PAT IP Address:	1.1.1.1
Filter Set...	<<None>>
Remove Filter Set	
Advanced IP Profile Options...	
COMMIT	CANCEL

- You must specify an **SPI (Security Parameters Index)**, which is the ESP receive side SPI and the default SPI for ESP transmit, AH receive, and AH transmit. It must be unique relative to any other configuration profile “ESP Receive SPIs.” (See [Advanced IP Profile Options on page 12-11.](#))
- You must specify a **Remote Tunnel Endpoint Address**. Specify the IP address of your tunnel partner, the endpoint of the tunnel. The Remote Tunnel Endpoint Address may be 0.0.0.0, which implies that the IPsec tunnel will not be established until packets are received on the SPI specified. At that time the tunnel will be bound to the Remote Tunnel Endpoint until traffic from the remote gateway ceases for a timeout period.
- You must specify a **Remote Members Network** address. This specifies the subnet of the remote IPsec tunnel and will be used with the Remote Members Mask to determine and set the route.
- You must specify a **Remote Members Mask**. This is the subnet mask of the remote subnet to which the IPsec tunnel will route.
- You can specify **Address Translation Enabled**. For more information see [Chapter 11, “Multiple Network Address Translation.”](#) If Address Translation Enabled is set to **Yes**, you can specify the following three fields:
 - **NAT Map List**
 - **NAT Server List**
 - **PAT IP Address**
(**Note:** Since there is no protocol to derive this address, 0.0.0.0 is not permitted.)

Map Lists, Server Lists, and PAT addresses are described in detail in [Chapter 11, “Multiple Network Address Translation.”](#)
- You can specify a **Filter Set**. See [About Filters and Filter Sets on page 13-4.](#)

- You can remove a **Filter Set**.
- You can choose to configure **Advanced IP Profile Options** (see “[Advanced IP Profile Options](#),” in the following section).

Note: The SPI title field above changes to **SPI (Security Parameters Index) – Use Advanced IP Profile Options** if any of the SPI values differ from each other.

Advanced IP Profile Options

Advanced IP Profile Options

ESP Receive SPI:	123456789
ESP Transmit SPI:	123456789
AH Receive SPI:	123456789
AH Transmit SPI:	123456789
Local Tunnel Endpoint Address:	0.0.0.0
Next Hop Gateway:	0.0.0.0

- You can specify an **ESP Receive SPI**. The value must be unique over the set of all ESP SPIs specified for the remote tunnel endpoint.
- You can specify an **ESP Transmit SPI**. The value must be unique over the set of all ESP SPIs specified for the remote tunnel endpoint.
- You can specify an **AH Receive SPI** if AH authentication has been requested. The value must be unique over the set of all AH SPIs specified for the router.
- You can specify an **AH Transmit SPI** if AH authentication has been requested. The value must be unique over the set of all AH SPIs specified for the remote tunnel endpoint.
- You can specify a **Local Tunnel Endpoint Address**. If not 0.0.0.0, this value must be one of the assigned interface addresses, either WAN or LAN. This is used as the source address of all IPsec traffic.
- You can specify a **Next Hop Gateway**. If you specify the Remote Tunnel Endpoint Address, and the address is in the same subnet as the Remote Members Network you specified in the IP Profile Parameters, the **Next Hop Gateway** option allows you to enter the address by which the gateway partner is reached.

If you do not specify the Remote Tunnel Endpoint Address, the router will use the default gateway to reach the partner. If the partner should be reached via an alternate port (for example, the LAN instead of the WAN), the **Next Hop Gateway** field allows this path to be resolved.

Interoperation with other features

- Address serving is not supported through IPsec Tunnels.
- AH is not supported through an interface that has NAT applied to it. NAT may be applied to the inner payload.
- AH is not supported through an interface which is either Unnumbered or Numbered with a dynamically assigned address unless the Local Tunnel Endpoint address is specified in the Advanced IP Profile Options screen.

Encryption Support

Encryption is a method for altering user data into a form that is unusable by anyone other than the intended recipient. The recipient must have the means to decrypt the data to render it usable to them. The encryption process protects the data by making it difficult for any third party to get at the original data.

Netopia PPTP is fully compatible with Microsoft Point-to-Point Encryption (MPPE) data encryption for user data transfer over the PPTP tunnel. Microsoft Windows NT Server provides MPPE encryption capability only when Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) is enabled. Netopia complies with this feature to allow MPPE only when MS-CHAP is negotiated. MS-CHAP and MPPE are user-selectable options in the PPTP Tunnel Options screen. If either the client or the server side specifies encryption, then encryption becomes mandatory for both.

Netopia's ATMP implementation supports Data Encryption Standard (DES) data encryption for user data transfer over the ATMP tunnel between two Netopia routers. The encryption option, none or DES, is a selectable option in the ATMP Tunnel Options screen.

MS-CHAP V2 and 128-bit strong encryption

Notes:

- The Netopia 4753 supports 128-bit ("strong") encryption when using PPTP tunnels.
ATMP does not have an option of using 128-bit MPPE. If you are using ATMP between two Netopia routers you can optionally set 56-bit DES encryption.
- When you choose MS-CHAP as the authentication method for a PPTP tunnel, the Netopia router will start negotiating MS-CHAPv2. If the router or VPN adapter client you are connecting to does not support MS-CHAPv2, the Netopia router will fall back to MS-CHAPv1, or, if the router or VPN adapter client you are connecting to does not support MPPE at all, the PPP session will be dropped. This is done automatically and transparently.

ATMP/PPTP Default Answer Profile

The WAN Configuration menu offers a ATMP/PPTP Default Answer Profile option. Use this selection when your router is acting as the server for VPN connections, that is, when you are on the answering end of the tunnel establishment. The ATMP/PPTP Default Answer Profile determines the way the attempted tunnel connection is answered.

```

                                WAN Configuration

                                WAN (Wide Area Network) Setup...
                                Display/Change Connection Profile...
                                Add Connection Profile...
                                Delete Connection Profile...

                                WAN Default Profile...
                                ATMP/PPTP Default Profile...
                                Scheduled Connections...

                                Configuration Changes Reset WAN Connection:      Yes
                                Frame Relay Configuration...
                                Frame Relay DLCI Configuration...

                                Establish WAN Connection...
                                Disconnect WAN Connection...

                                From here you will configure yours and the remote sites' WAN information.
  
```

To set the parameters under which the router will answer attempted VPN connections, select **ATMP/PPTP Default Answer Profile** and press Return. The Default VPN Profile screen appears.

```

                                ATMP/PPTP Default Profile

                                Answer VPN connections:                No

                                PPTP Configuration Options:
                                Receive Authentication...                PAP
                                Data Compression...                      None

                                Configure Default VPN Connection Parameters here.
  
```

- Toggle **Answer VPN Connections** to **Yes** if you want the router to accept VPN connections or **No** (the

default) if you do not. This applies to both ATMP and PPTP connections.

- For PPTP tunnel connections only, you must define what type of authentication these connections will use. Select **Receive Authentication** and press Return. A pop-up menu offers the following options: PAP (the default), CHAP, or MS-CHAP.
- If you chose PAP or CHAP authentication, from the **Data Compression** pop-up menu select either None (the default) or Standard LZS.

If you chose MS-CHAP authentication, the **Data Compression** option is not required, and this menu item becomes hidden.

VPN QuickView

You can view the status of your VPN connections in the VPN QuickView screen.

From the Main Menu select QuickView and then VPN QuickView.



The VPN QuickView screen appears.

VPN Quick View						
Profile Name-----	Type--	Rx Pckts--	Tx Pckts-----	Est.-	Partner Address-----	
HA <-> FA1 (Jony Fon	ATMP	99	99	Rmt	173.166.82.8	
HA <-> FA3 (Sleve M.	ATMP	13	14	Rmt	63.193.117.91	

Profile Name: Lists the name of the Connection Profile being used, if any.

Type: Shows the data link encapsulation method (PPTP or ATMP).

Rx Pckts: Shows the number of packets received via the VPN tunnel.

Tx Pckts: Shows the number of packets transmitted via the VPN tunnel.

Est: Indicates whether the connection was locally (“Lcl”) or remotely (“Rmt”) established.

Partner Address: Shows the tunnel partner’s IP address.

Dial-Up Networking for VPN

Microsoft Windows Dial-Up Networking software permits a remote standalone workstation to establish a VPN tunnel to a PPTP server such as a Netopia Router located at a central site. Dial-Up Networking also allows a mobile user who may not be connected to a PAC to dial into an intermediate ISP and establish a VPN tunnel to, for example, a corporate headquarters, remotely. Netopia Routers also can serve as a PAC at the workstation's site, making it unnecessary for the standalone workstation to initiate the tunnel. In such a case, the Dial-Up Networking software is not required, since the Netopia Router initiates the tunnel.

This section is provided for users who may require the VPN client software for Dial-Up Networking in order to connect to an ISP who provides a PPTP account.

Microsoft Windows Dial-Up Networking (DUN) is the means by which you can initiate a VPN tunnel between your individual remote client workstation and a private network such as your corporate LAN via the Internet. DUN is a software adapter that allows you to establish a tunnel.

DUN is a free add-on available for Windows 95, and comes standard with Windows 98 and Windows NT. The VPN tunnel behaves as a private network connection, unrelated to other traffic on the network. Once you have installed Dial-Up Networking, you will be able to connect to your remote site as if you had a direct private connection, regardless of the intervening network(s) through which your data passes. You may need to install the Dial-Up Networking feature of Windows 95, 98, or 2000 to take advantage of the virtual private networking feature of your Netopia router.

Note: For the latest information and tech notes on Dial-Up Networking and VPNs be sure to visit the Netopia website at <http://www.netopia.com> and, for the latest software and release notes, the Microsoft website at <http://www.microsoft.com>.

Installing PPTP and Configuring Dial-up Networking on a PPTP Client

Windows 98

1. From your Windows 98 desktop, go to the **Start Menu**, and select **Settings, Control Panel**, then double-click on **Add/Remove Programs**.
2. In the **Add/Remove Programs Properties** screen, select the **Windows Setup** tab.
3. In **Windows Setup** highlight and select **Communications** with a double-click of your mouse.
4. In **Communications**, under **Components**, make sure to check the boxes next to **Dial-up Networking** at the top of the list and **Virtual Private Networking** at the bottom of the list. Click **OK** at the bottom of each screen, then close the Control Panel screen by clicking the upper right corner marked with an **X**.

Note: Your Windows 98 Installation CD may be required, and your computer will need to be restarted.

5. Go to the **Start Menu** again, select **Programs**, select **Accessories**, select **Communications**, and click to select **Dial-up Networking**.
6. In **Dial-up Networking**, double-click on **Make New Connection**.
7. In the **Make New Connection** screen, follow the instructions by typing a name to identify your router, and select **Microsoft VPN Adapter** as your device. Click **Next**. Follow the instructions of the next screen and type the domain name or the public IP address of your router. Click **Next**, and then click **Finish**.

Note: The public IP address is the same as the router's Local WAN IP address if Address Translation (NAT) is enabled on your router, or if your router is configured for a Numbered interface. If NAT is not enabled, and your router is configured for an Unnumbered interface, you will enter the Ethernet IP address of your router. If your Local WAN IP address is assigned to you dynamically, check the Quick View menu of your routers console screen for the current WAN IP address.

8. Next, right click on the icon for the new Dial-Up Networking profile you just created and select **Properties**.
9. Select the **Server Types** tab of your connection profile window.
10. Confirm that **Log on to network** is unchecked. If you are using **MS-CHAP** in your router profile, then check **Require encrypted password**. If you selected the **MPPE** option for Data Encryption in your router's client connection profile (step 5 above), then you will need to have **Require data encryption** checked.

Windows NT 4.0

(The following information was obtained from the Microsoft's Windows NT Server White Paper titled "Installing, Configuring, and Using PPTP with Microsoft Clients and Servers.")

1. From your Windows NT desktop, go to the **Start Menu** and select **Settings, Control Panel**, then double-click **Network**.
2. In the **Network** screen, click the **Protocols** tab, and then click **Add** to display the **Select Network Protocol** dialog box.
3. Select **Point To Point Tunneling Protocol** and click **OK**.
4. Type the drive and directory location of your installation files in the **Windows NT Setup** dialog box, and then click **Continue**. The PPTP files are copied from the installation directory and the **PPTP Configuration** dialog box will appear.
5. Click the **Number of Virtual Private Networks** drop-down arrow and select the number of VPN devices you want the client to support. You can select a number between 1 and 256 for computers running Windows NT Workstation version 4.0 or Windows NT Server version 4.0. Typically, only one VPN is installed on a PPTP client.

Note: If the PPTP client is an ISP server running Windows NT Server version 4.0, you can select multiple VPN devices as needed to simultaneously support the PPP clients using the ISP server to connect to a PPTP server.

Click **OK**, and then click **OK** in the **Setup Message** dialog box.

6. In the **Remote Access Setup** properties dialog box, click **Add**.
7. Click the **RAS Capable Devices** list to display the VPN devices that must be added and configured as a port and device in RAS.
8. Select the **VPN1 - RASPPPM** device, and then click **OK**. (If you installed PPTP with more than one VPN device, repeat steps 7, 8 and 9 until all the VPNs are added to the **Remote Access Setup** properties dialog box.)
9. By default, the VPN device on a workstation running Windows NT 4.0 is configured to dial out only. Select the VPN port and click **Configure**. Verify that the **Dial out only** option in the **Port Usage** dialog box is the only option selected, and then click **OK**. This returns you to the **Remote Access Setup** properties dialog box.
10. Click **Network** to display the **Network Configuration** dialog box.

11. Verify that the **TCP/IP** option in **Dial out Protocols** is the only option checked, and then click **OK**.
12. Click **Continue**.
13. Close **Network**, shut down, and then restart your workstation.
14. Once your workstation has completely rebooted, go to the **Start Menu**, select **Accessories**, then click-on and select **Dial-up Networking**. (If this is the first phone book entry, a **Dial-up Networking** dialog box will appear. Click **OK**.)
15. Type a name to identify your router in the **Name the new phone book entry** field and click **Next**. Select **I am calling the Internet** and click **Next**. This configures the phone book entry to use TCP/IP and PPP as the Dial-up Networking protocols. Select **RASPPTPM(VPN1)** in the **Select the modem or adapter this entry will use** list in the **Modem or Adapter** dialog box, and then click **Next**. Type the domain name or the public IP address of your router in the **Phone Number** dialog box (see the Note in the step 6 of the previous section: Windows 98). Click **Next**, and then click **Finish**.
16. To verify or edit your phone book entry for the PPTP server, or your router, click **More** in **Dial-up Networking**, and then click **Edit entry and modem properties** to verify that your PPTP server phone book entry is correctly configured.
17. Review the information on the **Basic** tab to ensure that the phone number is correct and that the **RASPPTPM(VPN1)** device is selected. Make any necessary changes.
18. Click the **Server** tab. Review the information on the **Server** tab to ensure that the **Dial-up server type** displays **PPP: Windows NT, Windows 95 Plus, Internet**. In the **Network protocols** dialog box, ensure that the network protocols used on your private network are selected. Any selected protocol (TCP/IP, IPX/SPX, NetBEUI) must already be installed on the PPTP client your are configuring. In addition, RAS must be configured to use that protocol to dial out. Also, check the **TCP/IP Settings** to ensure that **Server assigned IP address** and **Server assigned name server addresses** are both selected. **Enable software compression** and **Enable PPP LCP extensions** should also be selected under the **Server** tab.
19. Click the **Script** tab, and then select **None**.
20. Click the **Security** tab. Click **Accept only Microsoft encrypted authentication**. The PPP protocol encrypts the user name and password for remote logon. If you are using the same name and password that you log into your computer with to authenticate with the router then select **Use current username and password**. If not, make sure this is unchecked.

Windows 2000

1. Right click on **My Network Places** and select **Properties**.
2. Select **Make New Connection** to start the **New Connection Wizard**. Click **Next**.
3. In the **Network Connection Type** window check **Connect to a Private Network through the Internet**; click **Next**.
4. In the **Public Network** dialog box: If you have a direct connection to the Internet, select **Do Not Dial the Initial Connection**, and click **Next**. If you have a Dial Up Networking connection that should be connected first, select **Automatically Dial this Initial Connection** and choose your Internet dial up from the pull down menu.
5. In the **Destination Address** window, type the **Local WAN IP** address of the router you are connecting to in the Host Name or IP Address field.

Note: If the router you are connecting to is not running NAT and has IP Addressing set to Unnumbered, there will be no Local WAN IP Address. In this case, use the Ethernet IP Address instead.

6. In the **Connection Availability** window, Windows will ask if you want all users to be able to use this VPN or just yourself. Select the choice that meets your network needs.
7. In the **Completing the Network Connection Wizard** menu, you will be prompted to name the connection. Assign a name that makes it easy for you to distinguish your connection. You can have Windows place a shortcut for this connection on your Desktop by checking the box at the bottom of the screen. Click **Finish**.
8. The connection will be prompted to dial. If you wish to connect, enter your User name and Password and click **Connect**. If not, click **Cancel**.

Windows ME

1. From your Windows ME desktop, go to the **Start Menu**, and select **Settings, Control Panel**, then double-click **Add/Remove Programs**.
2. In the **Add/Remove Programs Properties** screen, select the **Windows Setup** tab.
3. In **Windows Setup** highlight and select **Communications** with a double-click of your mouse.
4. In **Communications**, under **Components**, make sure to check the boxes next to **Dial-up Networking** at the top of the list and **Virtual Private Networking** at the bottom of the list. Click **OK** at the bottom of each screen, then close the Control Panel screen by clicking the upper right corner marked with an **X**.

Note: Your Windows ME Installation CD may be required, and your computer will need to be restarted.

5. Go to the **Start Menu** again, select **Programs**, select **Accessories**, select **Communications**, and click to select **Dial-up Networking**.
6. In **Dial-up Networking**, double-click on **Make New Connection**.
7. In the **Make New Connection** screen, follow the instructions by typing a name to identify your router, and select **Microsoft VPN Adapter** as your device. Click **Next**. Follow the instructions in the next screen and type the **Local WAN IP** address of the router you are connecting to in the **Host Name or IP Address** field.

Note: If the router you are connecting to is not running NAT and has IP Addressing set to Unnumbered, there will be no Local WAN IP Address. In this case, use the Ethernet IP Address instead.)

Click **Next**, and then click **Finish**.

8. Next, right click on the icon for the new **Dial-Up Networking profile** you just created and select **Properties**.
9. Select the **Security** tab of your connection profile window.
10. Confirm that **Log on to network** is unchecked. If you are using **MS-CHAP** in your router profile, then check **Require encrypted password**. If you selected the **MPPE** option for **Data Encryption** in your router's client connection profile (step 5 above), then you will need to have **Require data encryption** checked.

About ATMP Tunnels

To set up an ATMP tunnel, you create a Connection Profile including the IP address and other relevant information for the remote ATMP partner. ATMP uses the terminology of a *foreign agent* that initiates tunnels and a *home agent* that terminates them. You use the same procedure to initiate or terminate an ATMP tunnel. Used in this way, the terms *initiate* and *terminate* mean the beginning and end of the tunnel; they do not mean *activate* and *deactivate*.

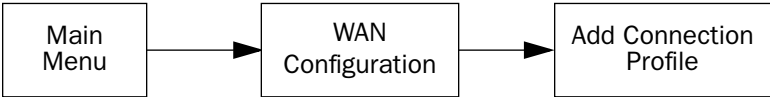
ATMP is a tunneling protocol, with two basic aspects. Tunnels are created and torn down using a session protocol that is UDP-based. User (or client) data is transferred across the tunnel by encapsulating the client data within Generic Routing Encapsulation (GRE). The GRE data is then routed using standard methods.

ATMP configuration

ATMP is a Datalink Encapsulation option in Connection Profiles. It is not an option in device or link configuration screens, since ATMP is not a native encapsulation. The Easy Setup Profile does not offer ATMP datalink encapsulation. See the *User's Reference Guide* for information on creating Connection Profiles.

The WAN Event History screens will report VPN tunnel events, such as connections and disconnections, as Channel 4 (and higher) events.

To define an ATMP tunnel, navigate to the **Add Connection Profile** menu from the Main Menu.



Add Connection Profile

Profile Name:

Profile Enabled:

Data Link Encapsulation...

Data Link Options...

IP Profile Parameters...

Profile 1

+-----+

+-----+

PPP

Frame Relay

ATM FUNI

ATMP

PPTP

+-----+

ADD PROFILE NOW

CANCEL

When you define a Connection Profile as using ATMP by selecting ATMP as the datalink encapsulation method, and then select **Data Link Options**, the ATMP Tunnel Options screen appears.

ATMP Tunnel Options	
ATMP Partner IP Address:	173.167.8.134
Tunnel Via Gateway:	0.0.0.0
Network Name:	sam.net
Password:	****
Data Encryption...	DES
Key String:	
Initiate Connections:	Yes
On Demand:	Yes
Idle Timeout (seconds):	300

Enter an IP address in decimal and dot form (xxx.xxx.xxx.xxx).
In this Screen you will configure the GRE/ATMP specific connection params.

Note: An ATMP tunnel cannot be assigned a dynamic IP address by the remote server, as in a PPP connection. When you define an ATMP tunnel profile, the Local WAN IP Address, assigned in the IP Profile Parameters screen, must be the true IP address, not 0.0.0.0, if NAT is enabled.

Profiles using ATMP do not offer a Telco Options screen.

- **ATMP Partner IP Address** specifies the address of the other end of the tunnel. When unspecified, the gateway can not initiate tunnels (i.e., act as a foreign agent) for this profile; it can only accept tunnel requests as a home agent.
- When you specify the ATMP Partner IP Address, and the address is in the same subnet as the Remote IP Address you specified in the IP Profile Parameters, you can specify the route (**Tunnel Via Gateway**) by which the gateway partner is reached. If you do not specify the ATMP Partner IP Address, the router will use the default gateway to reach the partner and the **Tunnel Via Gateway** field is hidden. If the partner should be reached via an alternate port (i.e., the LAN instead of the WAN), the **Tunnel Via Gateway** field allows this path to be resolved.
- You can specify a **Network Name**. When the tunnel partner is another Netopia router, this name may be used to match against a Connection Profile. When the partner is an Ascend router in Gateway mode, then **Network Name** is used by the Ascend router to match a gateway profile. When the partner is an Ascend router in Router mode, leave this field blank.
- You must specify a **Password**, used for authenticating the tunnel.
Note: The Password entry will be the same for both ends of the tunnel.
- For Netopia-to-Netopia connections only, you can specify a **Data Encryption** algorithm for the ATMP connection from the pop-up menu, either DES or None. None is the default.
Note: Ascend does not support DES encryption for ATMP tunnels.

- You must specify a **Key String** of up to (and including) 20 characters when DES is selected. When encryption is None, this field is invisible.
- You can specify that this router will **Initiate Connections**, acting as a foreign agent (**Yes**), or only answer them, acting as a home agent (**No**).
- Tunnels are normally initiated **On Demand**; however, you can disable this feature. When disabled, the tunnel must be manually established through the call management screens.
- You can specify the **Idle Timeout**, an inactivity timer, whose expiration will terminate the tunnel. A value of zero disables the timer. Because tunnels are subject to abrupt termination when the underlying datalink is torn down, use of the Idle Timeout is strongly encouraged.
- Return to the Connection Profile screen by pressing Escape.
- Select **IP Profile Parameters** and press Return. The IP Profile Parameters screen appears.

IP Profile Parameters

Address Translation Enabled:	Yes
NAT Map List...	Easy-PAT
NAT Server List...	Easy-Servers
Local WAN IP Address:	0.0.0.0
Remote IP Address:	173.167.8.10
Remote IP Mask:	255.255.0.0
Filter Set...	
Remove Filter Set	
Receive RIP:	Both

Enter a subnet mask in decimal and dot form (xxx.xxx.xxx.xxx).

- Enter the **Remote IP Address** and **Remote IP Mask** for the host to which you want to tunnel.

Allowing VPNs through a Firewall

An administrator interested in securing a network will usually combine the use of VPNs with the use of a firewall or some similar mechanism. This is because a VPN is not a complete security solution, but rather a component of overall security. Using a VPN will add security to transactions carried over a public network, but a VPN alone will not prevent a public network from infiltrating a private network. Therefore, you should combine use of a firewall with VPNs, where the firewall will secure the private network from infiltration from a public network, and the VPN will secure the transactions that must cross the public network.

A strict firewall may not be provisioned to allow VPN traffic to pass back and forth as needed. In order to ensure that a firewall will allow a VPN, certain attributes must be added to the firewall's provisioning. The provisions necessary vary slightly between ATMP and PPTP, but both protocols operate on the same basic premise: there are control and negotiation operations, and there is the tunnelled traffic that carries the payload of data between the VPN endpoints. The difference is that ATMP uses UDP to handle control and negotiation, while PPTP uses TCP. Then both ATMP and PPTP use GRE to carry the payload.

For PPTP negotiation to work, TCP packets inbound and outbound destined for port 1723 must be allowed. Likewise, for ATMP negotiation to work, UDP packets inbound and outbound destined for port 5150 must be allowed. Source ports are dynamic, so, if possible, make this flexible, too. Additionally, PPTP and ATMP both require a firewall to allow GRE bi-directionally.

The following sections illustrate a sample filtering setup to allow either PPTP or ATMP traffic to cross a firewall:

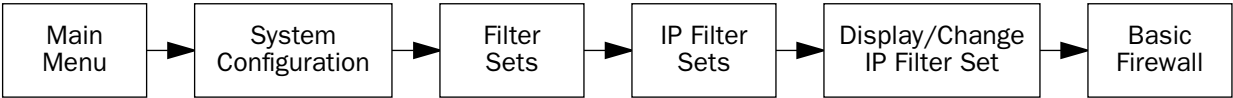
- [PPTP example on page 12-23](#)
- [ATMP example on page 12-26](#)

Make your own appropriate substitutions. For more information on filters and firewalls, see [Chapter 13, "Security."](#)

PPTP example

To enable a firewall to allow PPTP traffic, you must provision the firewall to allow inbound and outbound TCP packets specifically destined for port 1723. The source port may be dynamic, so often it is not useful to apply a compare function upon this portion of the control/negotiation packets. You must also set the firewall to allow inbound and outbound GRE packets, enabling transport of the tunnel payload.

From the Main Menu navigate to Display/Change IP Filter Set, and from the pop-up menu select **Basic Firewall**.



Select **Display/Change Input Filter**.

Display/Change Input Filter screen

+---#-----Source IP Addr-----Dest IP Addr-----Proto-Src.Port-D.Port--On?-Fwd--+									
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+									
1	0.0.0.0	0.0.0.0	TCP	NC	=1723	Yes	Yes		
2	0.0.0.0	0.0.0.0	GRE	--	--	Yes	Yes		

For Input Filter 1 set the Destination Port information as shown below.

Change Input Filter 1

Enabled:

Forward:

Yes

Yes

Source IP Address:

Source IP Address Mask:

0.0.0.0

0.0.0.0

Dest. IP Address:

Dest. IP Address Mask:

0.0.0.0

0.0.0.0

Protocol Type:

Source Port Compare...

Source Port ID:

Dest. Port Compare...

Dest. Port ID:

Established TCP Conns. Only:

TCP

No Compare

0

Equal

1723

No

For Input Filter 2 set the Protocol Type to allow GRE as shown below.

Change Input Filter 2

Enabled:

Yes

Forward:

Yes

Source IP Address:

0.0.0.0

Source IP Address Mask:

0.0.0.0

Dest. IP Address:

0.0.0.0

Dest. IP Address Mask:

0.0.0.0

Protocol Type:

GRE

In the Display/Change IP Filter Set screen select **Display/Change Output Filter**.

Display/Change Output Filter screen

+---#-----Source IP Addr-----Dest IP Addr-----Proto-Src.Port-D.Port--On?-Fwd--+									
+-----+-----+-----+-----+-----+-----+-----+-----+-----+									
1	0.0.0.0	0.0.0.0	TCP	NC	=1723	Yes	Yes		
2	0.0.0.0	0.0.0.0	GRE	--	--	Yes	Yes		

For Output Filter 1 set the Protocol Type and Destination Port information as shown below.

Change Output Filter 1

Enabled:

Yes

Forward:

Yes

Source IP Address:

0.0.0.0

Source IP Address Mask:

0.0.0.0

Dest. IP Address:

0.0.0.0

Dest. IP Address Mask:

0.0.0.0

Protocol Type:

TCP

Source Port Compare...

No Compare

Source Port ID:

0

Dest. Port Compare...

Equal

Dest. Port ID:

1723

Established TCP Conns. Only:

No

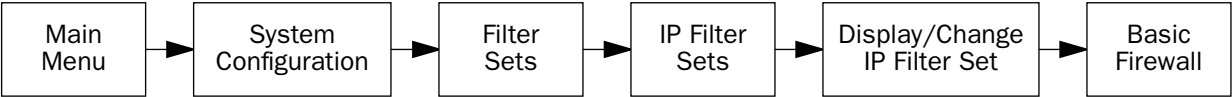
For Output Filter 2 set the Protocol Type to allow GRE as shown below.

Change Output Filter 2	
Enabled:	Yes
Forward:	Yes
Source IP Address:	0.0.0.0
Source IP Address Mask:	0.0.0.0
Dest. IP Address:	0.0.0.0
Dest. IP Address Mask:	0.0.0.0
Protocol Type:	GRE

ATMP example

To enable a firewall to allow ATMP traffic, you must provision the firewall to allow inbound and outbound UDP packets specifically destined for port 5150. The source port may be dynamic, so often it is not useful to apply a compare function on this portion of the control/negotiation packets. You must also set the firewall to allow inbound and outbound GRE packets (Protocol 47, Internet Assigned Numbers Document, RFC 1700), enabling transport of the tunnel payload.

From the Main Menu navigate to Display/Change IP Filter Set, and from the pop-up menu select **Basic Firewall**.



Select **Display/Change Input Filter**.

Display/Change Input Filter screen

+---#----Source IP Addr----Dest IP Addr-----Proto-Src.Port-D.Port--On?-Fwd--+									
+-----+-----+-----+-----+-----+-----+-----+-----+-----+									
1	0.0.0.0	0.0.0.0	UDP	NC	=5150	Yes	Yes		
2	0.0.0.0	0.0.0.0	GRE	--	--	Yes	Yes		

For Input Filter 1 set the Destination Port information as shown below.

Change Input Filter 1

Enabled:

Forward:

Source IP Address:

Source IP Address Mask:

Dest. IP Address:

Dest. IP Address Mask:

Protocol Type:

Source Port Compare...

Source Port ID:

Dest. Port Compare...

Dest. Port ID:

Established TCP Conns. Only:

Yes

Yes

0.0.0.0

0.0.0.0

0.0.0.0

0.0.0.0

TCP

No Compare

0

Equal

1723

No

For Input Filter 2 set the Protocol Type to allow GRE as shown below.

Change Input Filter 2

Enabled:

Forward:

Source IP Address:

Source IP Address Mask:

Dest. IP Address:

Dest. IP Address Mask:

Protocol Type:

Yes

Yes

0.0.0.0

0.0.0.0

0.0.0.0

0.0.0.0

GRE

In the Display/Change IP Filter Set screen select **Display/Change Output Filter**.

Display/Change Output Filter screen

+ #	Source IP Addr	Dest IP Addr	Proto	Src.Port	D.Port	On?	Fwd?
1	0.0.0.0	0.0.0.0	UDP	NC	NC	Yes	Yes
2	0.0.0.0	0.0.0.0	GRE	--	--	Yes	Yes

For Output Filter 1 set the Protocol Type and Destination Port information as shown below.

Change Output Filter 1

Enabled:

Forward:

Source IP Address:

Source IP Address Mask:

Dest. IP Address:

Dest. IP Address Mask:

Protocol Type:

Source Port Compare...

Source Port ID:

Dest. Port Compare...

Dest. Port ID:

Yes

Yes

0.0.0.0

0.0.0.0

0.0.0.0

0.0.0.0

UDP

No Compare

0

No Compare

5150

For Output Filter 2 set the Protocol Type to allow GRE as shown below.

Change Output Filter 2	
Enabled:	Yes
Forward:	Yes
Source IP Address:	0.0.0.0
Source IP Address Mask:	0.0.0.0
Dest. IP Address:	0.0.0.0
Dest. IP Address Mask:	0.0.0.0
Protocol Type:	GRE

Chapter 13

Security

The Netopia 4753 provides a number of security features to help protect its configuration screens and your local network from unauthorized access. Although these features are optional, it is strongly recommended that you use them.

This section covers the following topics:

- “Suggested Security Measures” on page 13-1
- “User Accounts” on page 13-1
- “Telnet Access” on page 13-3
- “About Filters and Filter Sets” on page 13-4
- “Working with IP Filters and Filter Sets” on page 13-11
- “Firewall Tutorial” on page 13-19
- “RADIUS Client Support” on page 13-30

Suggested Security Measures

In addition to setting up user accounts, Telnet access, and filters (all of which are covered later in this chapter), there are other actions you can take to make the Netopia 4753 and your network more secure:

- Change the SNMP community strings (or passwords). The default community strings are universal and could easily be known to a potential intruder.
- Set the answer profile so it must match incoming calls to a connection profile.
- Leave the Enable Dial-in Console Access option set to No.
- When using AURP, accept connections only from configured partners.
- Configure the Netopia 4753 through the serial console port to ensure that your communications cannot be intercepted.

User Accounts

When you first set up and configure the Netopia 4753, no passwords are required to access the configuration screens. Anyone could tamper with the router’s configuration by simply connecting it to a console.

However, by adding user accounts, you can protect the most sensitive screens from unauthorized access. User accounts are composed of name/password combinations that can be given to authorized users.

CAUTION! You are strongly encouraged to add protection to the configuration screens. Unprotected screens could allow an unauthorized user to compromise the operation of your entire network.

Once user accounts are created, users who attempt to access protected screens will be challenged. Users who enter an incorrect name or password are returned to a screen requesting a name/password combination to access the Main Menu.

To set up user accounts, in the System Configuration screen select **Security** and press Return. The Security Options screen appears.

Security Options

Enable Telnet Console Access:

Yes

Enable Telnet Access to SNMP Screens:

Yes

Console Access timeout (seconds):

600

Show Users...

Add User...

Delete User...

Advanced Security Options...

Password for This Screen (11 chars max):

Set up configuration access options here.

Protecting the Security Options screen

The first screen you should protect is the Security Options screen, because it controls access to the configuration screens. Access to the Security Options screen can be protected with a password.

Select **Password for This Screen** in the Security Options screen and enter a password. Make sure this password is secure and is different from any of the user account passwords.

Protecting the configuration screens

You can protect the configuration screens with user accounts. You can administer the accounts from the Security Options screen. You can create up to four accounts.

To display a view-only list of user accounts, select **Show Users** in the Security Options screen.

To add a new user account, select **Add User** in the Security Options screen and press Return. The Add Name With Write Access screen appears.

Add Name With Write Access

Enter Name:

Enter Password (11 characters max):

ADD NAME/PASSWORD NOWCANCEL

Follow these steps to configure the new account:

1. Select **Enter Name** and enter a descriptive name (for example, the user's first name).
2. Select **Enter Password** and enter a password.
3. To accept the new name/password combination, select **ADD NAME/PASSWORD NOW** and press Return. To exit the Add Name With Write Access screen without saving the new account, select **CANCEL**. You are returned to the Security Options screen.

To delete a user account, select **Delete User** to display a list of accounts. Select an account from the list and press Return to delete it. To exit the list without deleting the selected account, press Escape.

Telnet Access

Telnet is a TCP/IP service that allows remote terminals to access hosts on an IP network. The Netopia 4753 supports Telnet access to its configuration screens.

CAUTION! You should consider password-protecting or restricting Telnet access to the Netopia 4753 if you suspect there is a chance of tampering.

To password-protect the configuration screens, select Easy Setup from the Main Menu, and go to the Easy Setup Security Configuration screen. By entering a name and password pair in this screen, all access via serial, Telnet, SNMP, and Web server will be password-protected.

To restrict Telnet access, select **Security** in the Advanced Configuration menu. The Security Options screen will appear. There are two levels of Telnet restriction available:

- To restrict Telnet access to the SNMP screens, select **Enable Telnet Access to SNMP Screens** and toggle

it to **No**. (See “SNMP traps” on page 14-15.)

- To restrict Telnet access to all of the configuration screens, select **Enable Telnet Console Access** and toggle it to **No**.

About Filters and Filter Sets

Security should be a high priority for anyone administering a network connected to the Internet. Using packet filters to control network communications can greatly improve your network’s security.

The Netopia 4753’s packet filters are designed to provide security for the Internet connections made to and from your network. You can customize the router’s filter sets for a variety of packet filtering applications. Typically, you use filters to selectively admit or refuse TCP/IP connections from certain remote networks and specific hosts. You will also use filters to screen particular types of connections. This is commonly called firewalling your network.

Before creating filter sets, you should read the next few sections to learn more about how these powerful security tools work.

What’s a filter and what’s a filter set?

A filter is a rule that lets you specify what sort of data can flow in and out of your network. A particular filter can be either an input filter—one that is used on data (packets) coming in to your network from the Internet—or an output filter—one that is used on data (packets) going out from your network to the Internet.

A filter set is a group of filters that work together to check incoming or outgoing data. A filter set can consist of a combination of input and output filters.

How filter sets work

A filter set acts like a team of customs inspectors. Each filter is an inspector through which incoming and outgoing packages must pass. The inspectors work as a team, but each inspects every package individually.

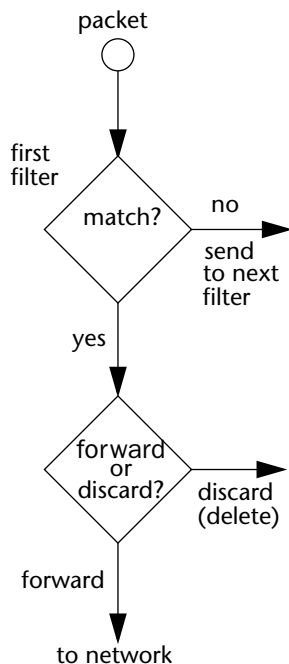
Each inspector has a specific task. One inspector’s task may be to examine the destination address of all outgoing packages. That inspector looks for a certain destination—which could be as specific as a street address or as broad as an entire country—and checks each package’s destination address to see if it matches that destination.



A filter inspects data packets like a customs inspector scrutinizing packages.

Filter priority

Continuing the customs inspectors analogy, imagine the inspectors lined up to examine a package. If the package matches the first inspector's criteria, the package is either rejected or passed on to its destination, depending on the first inspector's particular orders. In this case, the package is never seen by the remaining inspectors.



If the package does not match the first inspector's criteria, it goes to the second inspector, and so on. You can see that the order of the inspectors in the line is very important.

For example, let's say the first inspector's orders are to send along all packages that come from Rome, and the second inspector's orders are to reject all packages that come from France. If a package arrives from Rome, the first inspector sends it along without allowing the second inspector to see it. A package from Paris is ignored by the first inspector, rejected by the second inspector, and never seen by the others. A package from London is ignored by the first two inspectors, so it's seen by the third inspector.

In the same way, filter sets apply their filters in a particular order. The first filter applied can forward or discard a packet before that packet ever reaches any of the other filters. If the first filter can neither forward nor discard the packet (because it cannot match any criteria), the second filter has a chance to forward or reject it, and so on. Because of this hierarchical structure, each filter is said to have a priority. The first filter has the highest priority, and the last filter has the lowest priority.

How individual filters work

As described above, a filter applies criteria to an IP packet and then takes one of three actions:

- Forwards the packet to the local or remote network
- Blocks (discards) the packet
- Ignores the packet

A filter forwards or blocks a packet only if it finds a match after applying its criteria. When no match occurs, the filter ignores the packet.

A filtering rule

The criteria are based on information contained in the packets. A filter is simply a rule that prescribes certain actions based on certain conditions. For example, the following rule qualifies as a filter:

Block all Telnet attempts that originate from the remote host 199.211.211.17.

This rule applies to Telnet packets that come from a host with the IP address 199.211.211.17. If a match occurs, the packet is blocked.

Here is what this rule looks like when implemented as a filter on the Netopia 4753:

+ -# - -	Source IP Addr	- -Dest IP Addr	- - - - -Proto	- Src.Port	- D.Port	- -On?	- Fwd	- +
1	199.211.211.17	0.0.0.0	TCP	23		Yes	No	

To understand this particular filter, look at the parts of a filter.

Parts of a filter

A filter consists of criteria based on packet attributes. A typical filter can match a packet on any one of the following attributes:

- The source IP address (where the packet was sent from)
- The destination IP address (where the packet is going)
- The type of higher-layer Internet protocol the packet is carrying, such as TCP or UDP

Port numbers

A filter can also match a packet’s port number attributes, but only if the filter’s protocol type is set to TCP or UDP, since only those protocols use port numbers. The filter can be configured to match the following:

- The source port number (the port on the sending host that originated the packet)
- The destination port number (the port on the receiving host that the packet is destined for)

By matching on a port number, a filter can be applied to selected TCP or UDP services, such as Telnet, FTP, and World Wide Web. The following tables show a few common services and their associated port numbers:

Internet service	TCP port	Internet service	TCP port
FTP	20/21	Finger	79
Telnet	23	World Wide Web	80
SMTP (mail)	25	News	144
Gopher	70	rlogin	513

Internet service	UDP port	Internet service	UDP port
Who Is	43	AppleTalk Routing Maintenance (at-rtmp)	202
World Wide Web	80	AppleTalk Name Binding (at-nbp)	202
SNMP	161	AURP (AppleTalk)	387
TFTP	69	who	513

Port number comparisons

A filter can also use a comparison option to evaluate a packet's source or destination port number. The comparison options are:

No Compare: No comparison of the port number specified in the filter with the packet's port number.

Not Equal To: For the filter to match, the packet's port number cannot equal the port number specified in the filter.

Less Than: For the filter to match, the packet's port number must be less than the port number specified in the filter.

Less Than or Equal: For the filter to match, the packet's port number must be less than or equal to the port number specified in the filter.

Equal: For the filter to match, the packet's port number must equal the port number specified in the filter.

Greater Than: For the filter to match, the packet's port number must be greater than the port number specified in the filter.

Greater Than or Equal: For the filter to match, the packet's port number must be greater than or equal to the port number specified in the filter.

Other filter attributes

There are three other attributes to each filter:

- The filter’s order (i.e., priority) in the filter set
- Whether the filter is currently active
- Whether the filter is set to forward packets or to block (discard) packets

Putting the parts together

When you display a filter set, its filters are displayed as rows in a table:

+-#	---Source IP Addr	---Dest IP Addr	-----Proto	Src.Port	D.Port	--On?	-Fwd-
1	192.211.211.17	0.0.0.0	TCP	0	23	Yes	No
2	0.0.0.0	0.0.0.0	TCP	NC	=6000	Yes	No
3	0.0.0.0	0.0.0.0	ICMP	--	--	Yes	Yes
4	0.0.0.0	0.0.0.0	TCP	NC	>1023	Yes	Yes
5	0.0.0.0	0.0.0.0	UDP	NC	>1023	Yes	Yes

The table’s columns correspond to each filter’s attributes:

#: The filter’s priority in the set. Filter number 1, with the highest priority, is first in the table.

Source IP Addr: The packet source IP address to match.

Dest IP Addr: The packet destination IP address to match.

Proto: The protocol to match. This can be entered as a number (see the table below) or as TCP or UDP if those protocols are used.

Protocol	Number to use	Full name
N/A	0	Ignores protocol type
ICMP	1	Internet Control Message Protocol
TCP	6	Transmission Control Protocol
UDP	17	User Datagram Protocol

Src. Port: The source port to match. This is the port on the sending host that originated the packet.

D. Port: The destination port to match. This is the port on the receiving host for which the packet is intended.

On?: Displays **Yes** when the filter is in effect or **No** when it is not.

Fwd: Shows whether the filter forwards (**Yes**) a packet or discards (**No**) it when there's a match.

Filtering example #1

Returning to our filtering rule example from above (see [page 13-6](#)), look at how a rule is translated into a filter. Start with the rule, then fill in the filter's attributes:

1. The rule you want to implement as a filter is:

Block all Telnet attempts that originate from the remote host 199.211.211.17.

2. The host 199.211.211.17 is the source of the Telnet packets you want to block, while the destination address is any IP address. How these IP addresses are masked determines what the final match will be, although the mask is not displayed in the table that displays the filter sets (you set it when you create the filter). In fact, since the mask for the destination IP address is 0.0.0.0, the address for Dest IP Addr could have been anything. The mask for Source IP Addr must be 255.255.255.255 since an exact match is desired.

- Source IP Addr = 199.211.211.17
- Source IP address mask = 255.255.255.255
- Dest IP Addr = 0.0.0.0
- Destination IP address mask = 0.0.0.0

Note: To learn about IP addresses and masks, see [Appendix B, "Understanding IP Addressing."](#)

3. Using the tables on [page 13-7](#), find the destination port and protocol numbers (the *local* Telnet port):

- Proto = TCP (or 6)
- D. Port = 23

4. The filter should be enabled and instructed to block the Telnet packets containing the source address shown in step 2:

- On? = Yes
- Fwd = No

This four-step process is how we produced the following filter from the original rule:

+	#	---	Source IP Addr	---	Dest IP Addr	----	Proto	Src.Port	D.Port	--	On?	Fwd	+
1			192.211.211.17		0.0.0.0		TCP	0	23		Yes	No	

- Filters are complex. Combining them in filter sets introduces subtle interactions, increasing the likelihood of implementation errors.
- Enabling a large number of filters can have a negative impact on performance. Processing of packets will take longer if they have to go through many checkpoints.
- Too much reliance on packet filters can cause too little reliance on other security methods. Filter sets are *not* a substitute for password protection, effective safeguarding of passwords, caller ID, the “must match”

option in the answer profile, PAP or CHAP in connection profiles, callback, and general awareness of how your network may be vulnerable.

An approach to using filters

The ultimate goal of network security is to prevent unauthorized access to the network without compromising authorized access. Using filter sets is part of reaching that goal.

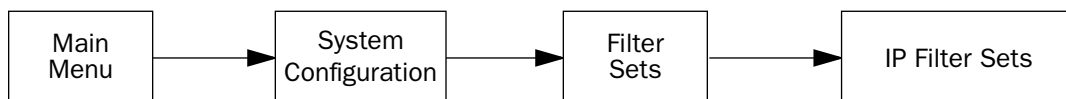
Each filter set you design will be based on one of the following approaches:

- That which is not expressly prohibited is permitted.
- That which is not expressly permitted is prohibited.

It is strongly recommended that you take the latter, and safer, approach to all of your filter set designs.

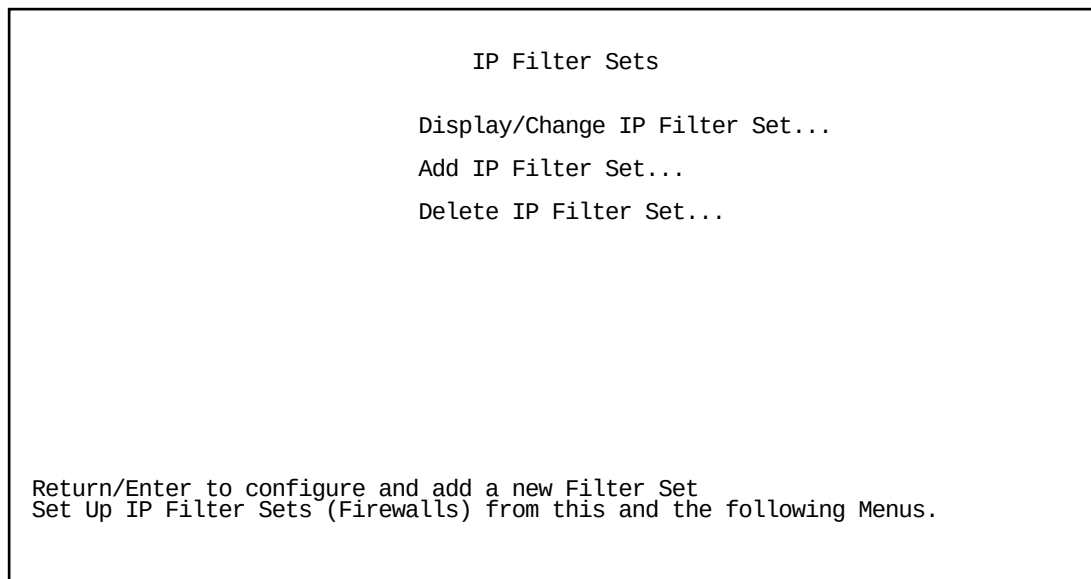
Working with IP Filters and Filter Sets

This section covers IP filters and filter sets.



To work with filters and filter sets, begin by accessing the filter set screens.

Note: Make sure you understand how filters work before attempting to use them. Read the section [“About Filters and Filter Sets,” beginning on page 13-4.](#)



The procedure for creating and maintaining filter sets is as follows:

13-12 Administration Guide

1. Add a new filter set.
2. Create the filters for the new filter set.
3. View, change, or delete individual filters and filter sets.

The sections below explain how to execute these steps.

Adding a filter set

You can create up to eight different custom filter sets. Each filter set can contain up to 256 filters. For more information, refer to Netopia Tech Notes NIR_052 and NIR_066 found on the Netopia website.

To add a new filter set, select **Add IP Filter Set** in the IP Filter Sets screen and press Return. The Add Filter Set screen appears.

Note: There are two groups of items in the Add IP Filter Set screen, one for input filters and one for output filters. The two groups work in essentially the same way, as you'll see below.

Add IP Filter Set

Filter Set Name:Filter Set 3

Display/Change Input Filter...

Add Input Filter...

Delete Input Filter...

Display/Change Output Filter...

Add Output Filter...

Delete Output Filter...

ADD FILTER SET

CANCEL

Configure the Filter Set name and its associated Filters.

Naming a new filter set

All new filter sets have a default name. The first filter set you add will be called Filter Set 1, the next filter will be Filter Set 2, and so on.

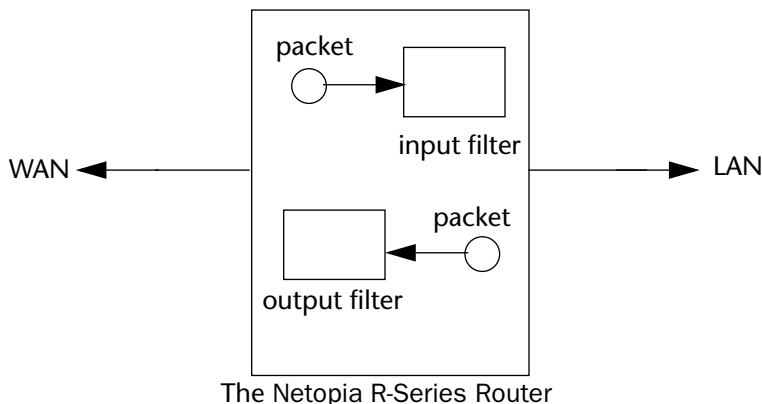
To give a new filter set a different name, select **Filter Set Name** and enter a new name for the filter set.

To save the filter set, select **ADD FILTER SET**. The saved filter set is empty (contains no filters), but you can return to it later to add filters (see [“Modifying filter sets” on page 13-16](#)). Or you can add filters to your new set before saving it (see [“Adding filters to a filter set” on page 13-13](#)).

To leave the Add Filter Set screen without saving the new filter set select **CANCEL**. You are returned to the IP Filter Sets screen.

Input and output filters—source and destination

There are two kinds of filters you can add to a filter set: input and output. Input filters check packets received from the Internet, destined for your network. Output filters check packets transmitted from your network to the Internet.



Packets in the Netopia 4753 pass through an input filter if they originate in the WAN and through an output filter if they're being sent out to the WAN.

The process for adding input and output filters is exactly the same. The main difference between the two involves their reference to source and destination. From the perspective of an input filter, your local network is the destination of the packets it checks, and the remote network is their source. From the perspective of an output filter, your local network is the source of the packets, and the remote network is their destination.

Type of filter	Source means	Destination means
Input filter	The remote network	The local network
Output filter	The local network	The remote network

Adding filters to a filter set

In this section you'll learn how to add an input filter to a filter set. Adding an output filter works exactly the same way, providing you keep the different source and destination perspectives in mind.

To add an input filter, select **Add Input Filter** in the Add IP Filter Set screen. The Add Filter screen appears. (To add an output filter, select **Add Output Filter**.)

Add Filter	
Enabled:	No
Forward:	No
Source IP Address:	0.0.0.0
Source IP Address Mask:	0.0.0.0
Dest. IP Address:	0.0.0.0
Dest. IP Address Mask:	0.0.0.0
Protocol Type:	0
Source Port Compare...	No Compare
Source Port ID:	0
Dest. Port Compare...	No Compare
Dest. Port ID:	0
ADD THIS FILTER NOW	CANCEL

Enter the IP specific information for this filter.

1. To make the filter active in the filter set, select **Enabled** and toggle it to **Yes**. If **Enabled** is toggled to **No**, the filter can still exist in the filter set, but it will have no effect.
 2. If you want the filter to forward packets that match its criteria to the destination IP address, select **Forward** and toggle it to **Yes**. If **Forward** is toggled to **No**, packets matching the filter's criteria will be discarded.
 3. Select **Source IP Address** and enter the source IP address this filter will match on. You can enter a subnet or a host address.
 4. Select **Source IP Address Mask** and enter a mask for the source IP address. This allows you to further modify the way the filter will match on the source address. Enter 0.0.0.0 to force the filter to match on all source IP addresses, or enter 255.255.255.255 to match the source IP address exclusively.
 5. Select **Dest. IP Address** and enter the destination IP address this filter will match on. You can enter a subnet or a host address.
 6. Select **Dest. IP Address Mask** and enter a mask for the destination IP address. This allows you to further modify the way the filter will match on the destination address. Enter 0.0.0.0 to force the filter to match on all destination IP addresses.
 7. Select **Protocol Type** and enter **ICMP**, **TCP**, **UDP**, **Any**, or the number of another IP transport protocol (see the table on [page 13-8](#)).
- Note:** If Protocol Type is set to TCP or UDP, the settings for port comparison that you configure in steps 8 and 9 will appear. These settings only take effect if the Protocol Type is TCP or UDP.
8. Select **Source Port Compare** and choose a comparison method for the filter to use on a packet's source port number. Then select **Source Port ID** and enter the actual source port number to match on (see the table on [page 13-7](#)).
 9. Select **Dest. Port Compare** and choose a comparison method for the filter to use on a packet's destination port number. Then select **Dest. Port ID** and enter the actual destination port number to match on (see the table on [page 13-7](#)).

10. When you are finished configuring the filter, select **ADD THIS FILTER NOW** to save the filter in the filter set. Select **CANCEL** to discard the filter and return to the Add IP Filter Set screen.

Viewing filters

To display a view-only table of input or output filters, select **Display/Change Input Filter** or **Display/Change Output Filter** in the Add IP Filter Set screen.

Modifying filters

To modify a filter, select **Display/Change Input Filter** or **Display/Change Output Filter** in the Add IP Filter Set screen to display a table of filters.

Select a filter from the table and press Return. The Change Filter screen appears. The parameters in this screen are set in the same way as the ones in the Add Filter screen (see [“Adding filters to a filter set” on page 13-13](#)).

Change Filter	
Enabled:	No
Forward:	No
Source IP Address:	0.0.0.0
Source IP Address Mask:	0.0.0.0
Dest. IP Address:	0.0.0.0
Dest. IP Address Mask:	0.0.0.0
Protocol Type:	0
Source Port Compare...	No Compare
Source Port ID:	0
Dest. Port Compare...	No Compare
Dest. Port ID:	0

Enter the IP specific information for this filter.

Deleting filters

To delete a filter, select **Delete Input Filter** or **Delete Output Filter** in the Add IP Filter Set screen to display a table of filters.

Select the filter from the table and press Return to delete it. Press Escape to exit the table without deleting the filter.

Viewing filter sets

To display a view-only list of filter sets, select **Display/Change IP Filter Set** in the IP Filter Sets screen.

Modifying filter sets

To modify a filter set, select **Display/Change IP Filter Set** in the IP Filter Sets screen to display a list of filter sets.

Select a filter set from the list and press Return. The Change IP Filter Set screen appears. The items in this screen are the same as the ones in the Add Filter screen (see [“Adding filters to a filter set” on page 13-13](#)).

Change IP Filter Set

Filter Set Name: Basic Firewall

Display/Change Input Filter...

Add Input Filter...

Delete Input Filter...

Display/Change Output Filter...

Add Output Filter...

Delete Output Filter...

Deleting a filter set

Note: If you delete a filter set, all of the filters it contains are deleted as well. To reuse any of these filters in another set, before deleting the current filter set you'll have to note their configuration and then recreate them.

To delete a filter set, select **Delete IP Filter Set** in the IP Filter Sets screen to display a list of filter sets.

Select a filter set from the list and press Return to delete it. Press Escape to exit the list without deleting the filter set.

A sample IP filter set

This section contains the settings for a filter set called Basic Firewall, which is part of the Netopia 4753's factory configuration.

Basic Firewall blocks undesirable traffic originating from the WAN (in most cases, the Internet), but forwards all traffic originating from the LAN. It follows the conservative “that which is not expressly permitted is prohibited” approach: unless an incoming packet expressly matches one of the constituent input filters, it will not be forwarded to the LAN.

The five input filters and one output filter that make up Basic Firewall are shown in the table below.

Setting	Input filter 1	Input filter 2	Input filter 3	Input filter 4	Input filter 5	Output filter 1
Enabled	Yes	Yes	Yes	Yes	Yes	Yes
Forward	No	No	Yes	Yes	Yes	Yes
Source IP address	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Source IP address mask	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Dest. IP address	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Dest. IP address mask	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Protocol type	TCP	TCP	ICMP	TCP	UDP	0
Source port comparison	No Compare	No Compare	N/A	No Compare	No Compare	N/A
Source port ID	0	0	N/A	0	0	N/A
Dest. port comparison	Equal	Equal	N/A	Greater Than	Greater Than	N/A
Dest. port ID	2000	6000	N/A	1023	1023	N/A

Basic Firewall's filters play the following roles.

Input filters 1 and 2: These block WAN-originated OpenWindows and X-Windows sessions. Service origination requests for these protocols use ports 2000 and 6000, respectively. Since these are greater than 1023, OpenWindows and X-Windows traffic would otherwise be allowed by input filter 4. Input filters 1 and 2 must precede input filter 4; otherwise they would have no effect since filter 4 would have already forwarded OpenWindows and X-Windows traffic.

Input filter 3: This filter explicitly forwards all WAN-originated ICMP traffic to permit devices on the WAN to ping devices on the LAN. Ping is an Internet service that is useful for diagnostic purposes.

Input filters 4 and 5: These filters forward all TCP and UDP traffic, respectively, when the destination port is greater than 1023. This type of traffic generally does not allow a remote host to connect to the LAN using one of the potentially intrusive Internet services, such as Telnet, FTP, and WWW.

Output filter 1: This filter forwards all outgoing traffic to make sure that no outgoing connections from the LAN are blocked.

13-18 Administration Guide

Basic Firewall is suitable for a LAN containing only client hosts that want to access servers on the WAN, but not for a LAN containing servers providing services to clients on the WAN. Basic Firewall's general strategy is to explicitly forward WAN-originated TCP and UDP traffic to ports greater than 1023. Ports lower than 1024 are the service origination ports for various Internet services such as FTP, Telnet, and the World Wide Web (WWW).

A more complicated filter set would be required to provide WAN access to a LAN-based server. See the next section, "[Possible modifications](#)," for ways to allow remote hosts to use services provided by servers on the LAN.

Possible modifications

You can modify the sample filter set Basic Firewall to allow incoming traffic using the examples below. These modifications are not intended to be combined. Each modification is to be the only one used with Basic Firewall.

The results of combining filter set modifications can be difficult to predict. It is recommended that you take special care if you are making more than one modification to the sample filter set.

Trusted host. To allow unlimited access by a trusted remote host with the IP address a.b.c.d (corresponding to a numbered IP address such as 163.176.8.243), insert the following input filter ahead of the current input filter 1:

- Enabled: Yes
- Forward: Yes
- Source IP Address: a.b.c.d
- Source IP Address Mask: 255.255.255.255
- Dest. IP Address: 0.0.0.0
- Dest. IP Address Mask: 0.0.0.0
- Protocol Type: 0

Trusted subnet. To allow unlimited access by a trusted remote subnet with subnet address a.b.c.d (corresponding to a numbered IP address such as 163.176.8.0) and subnet mask e.f.g.h (corresponding to a numbered IP mask such as 255.255.255.0), insert the following input filter ahead of the current input filter 1:

- Enabled: Yes
- Forward: Yes
- Source IP Address: a.b.c.d
- Source IP Address Mask: e.f.g.h
- Dest. IP Address: 0.0.0.0
- Dest. IP Address Mask: 0.0.0.0
- Protocol Type: 0

FTP sessions. To allow WAN-originated FTP sessions to a LAN-based FTP server with the IP address a.b.c.d (corresponding to a numbered IP address such as 163.176.8.243), insert the following input filter ahead of the current input filter 1:

- Enabled: Yes
- Forward: Yes
- Source IP Address: 0.0.0.0
- Source IP Address Mask: 0.0.0.0
- Dest. IP Address: a.b.c.d
- Dest. IP Address Mask: 255.255.255.255
- Protocol Type: TCP
- Source Port Comparison: No Compare
- Source Port ID: 0
- Dest. Port Comparison: Equal
- Dest. Port ID: 21

Note: A similar filter could be used to permit Telnet or WWW access. Set the Dest. Port ID to 23 for Telnet or to 80 for WWW.

Deleting a filter set does not delete the filters in that set. However, the filters in the deleted set are no longer in effect (unless they are part of another set). The deleted set will no longer appear in the answer profile or any connection profiles to which it was added.

Firewall Tutorial

General firewall terms

Filter rule: A filter set is comprised of individual filter rules.

Filter set: A grouping of individual filter rules.

Firewall: A component or set of components that restrict access between a protected network and the Internet, or between two networks.

Host: A workstation on the network.

Packet: Unit of communication on the Internet.

Packet filter: Packet filters allow or deny packets based on source or destination IP addresses, TCP or UDP ports, or the TCP ACK bit.

Port: A number that defines a particular type of service.

Basic IP packet components

All IP packets contain the same basic header information, as follows:

Source IP Address	163.176.132.18
Destination IP Address	163.176.4.27
Source Port	2541
Destination Port	80
Protocol	TCP
ACK Bit	Yes
DATA	User Data

This header information is what the packet filter uses to make filtering decisions. It is important to note that a packet filter does not look into the IP data stream (the User Data from above) to make filtering decisions.

Basic protocol types

- TCP:** Transmission Control Protocol. TCP provides reliable packet delivery and has a retransmission mechanism (so packets are not lost). RFC 793 is the specification for TCP.
- UDP:** User Datagram Protocol. Unlike TCP, UDP does not guarantee reliable, sequenced packet delivery. If data does not reach its destination, UDP does not retransmit the data. RFC 768 is the specification for UDP.

There are many more ports defined in the Assigned Addresses RFC. The table that follows shows some of these port assignments.

Example TCP/UDP Ports

TCP Port	Service
20/21	FTP
23	Telnet
25	SMTP
80	WWW
144	News

UDP Port	Service
161	SNMP

UDP Port	Service
69	TFTP
387	AURP

Firewall design rules

There are two basic rules to firewall design:

- “What is not explicitly allowed is denied.”

and

- “What is not explicitly denied is allowed.”

The first rule is far more secure, and is the best approach to firewall design. It is far easier (and more secure) to allow in or out only certain services and deny anything else. If the other rule is used, you would have to figure out everything that you want to disallow, now and in the future.

Firewall Logic

Firewall design is a test of logic, and filter rule ordering is critical. If a packet is forwarded through a series of filter rules and then the packet matches a rule, the appropriate action is taken. The packet will not forward through the remainder of the filter rules.

For example, if you had the following filter set...

Allow WWW access;
 Allow FTP access;
 Allow SMTP access;
 Deny all other packets.

and a packet goes through these rules destined for FTP, the packet would forward through the first rule (WWW), go through the second rule (FTP), and match this rule; the packet is allowed through.

If you had this filter set for example....

Allow WWW access;
 Allow FTP access;
 Deny FTP access;
 Deny all other packets.

and a packet goes through these rules destined for FTP, the packet would forward through the first filter rule (WWW), match the second rule (FTP), and the packet is allowed through. Even though the next rule is to deny all FTP traffic, the FTP packet will never make it to this rule.

Binary representation

It is easiest when doing filtering to convert the IP address and mask in question to binary. This will allow you to perform the logical AND to determine whether a packet matches a filter rule.

Logical AND function

When a packet is compared (in most cases) a logical AND function is performed. First the IP addresses and subnet masks are converted to binary and then combined with AND. The rules for the logical use of AND are as follows:

- 0 AND 0 = 0
- 0 AND 1 = 0
- 1 AND 0 = 0
- 1 AND 1 = 1

For example:

Filter rule:

Deny
IP: 163.176.1.15BINARY: 10100011.10110000.00000001.00001111
Mask: 255.255.255.255BINARY:11111111.11111111.11111111.11111111

Incoming Packet:

IP 163.176.1.15BINARY: 10100011.10110000.00000001.00001111

If you put the incoming packet and subnet mask together with AND, the result is:

10100011.10110000.00000001.00001111

which matches the IP address in the filter rule and the packet is denied.

Implied rules

With a given set of filter rules, there is an Implied rule that may or may not be shown to the user. The implied rule tells the filter set what to do with a packet that does not match any of the filter rules. An example of implied rules is as follows:

Implied	Meaning
Y+Y+Y=N	If all filter rules are YES, the implied rule is NO.
N+N+N=Y	If all filter rules are NO, the implied rule is YES.
Y+N+Y=N	If a mix of YES and NO filters, the implied rule is NO.

Established connections

The TCP header contains one bit called the ACK bit (or TCP Ack bit). This ACK bit appears only with TCP, not UDP. The ACK bit is part of the TCP mechanism that guarantees the delivery of data. The ACK bit is set whenever one side of a connection has received data from the other side. Only the first TCP packet will not have the ACK bit set; once the TCP connection is in place, the remainder of the TCP packets will have the ACK bit set.

The ACK bit is helpful for firewall design and reduces the number of potential filter rules. A filter rule could be created just allowing incoming TCP packets with the ACK bit set, since these packets had to be originated from the local network.

Example IP filter set screen

This is an example of the Netopia IP filter set screen:

Change Filter

Enabled:

Yes

Forward:

No

Source IP Address:

0.0.0.0

Source IP Address Mask:

0.0.0.0

Dest. IP Address:

0.0.0.0

Dest. IP Address Mask:

0.0.0.0

Protocol Type:

TCP

Source Port Compare...

No Compare

Source Port ID:

0

Dest. Port Compare...

Equal

Dest. Port ID:

2000

Established TCP Conns. Only:

No

Return/Enter accepts * Tab toggles * ESC cancels.

Enter the IP specific information for this filter.

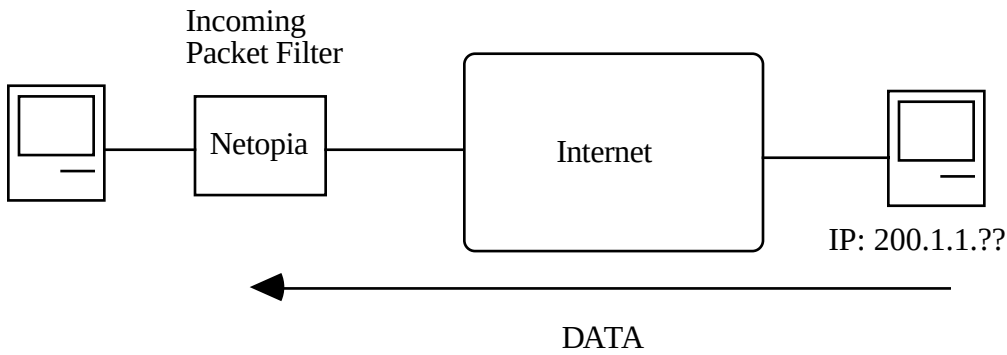
Filter basics

In the source or destination IP address fields, the IP address that is entered must be the network address of the subnet. A host address can be entered, but the applied subnet mask must be 32 bits (255.255.255.255).

The Netopia 4753 has the ability to compare source and destination TCP or UDP ports. These options are as follows:

Item	What it means
No Compare	Does not compare TCP or UDP port
Not Equal To	Matches any port other than what is defined
Less Than	Anything less than the port defined
Less Than or Equal	Any port less than or equal to the port defined
Equal	Matches only the port defined
Greater Than or Equal	Matches the port or any port greater
Greater Than	Matches anything greater than the port defined

Example network



Example filters

Example 1

Filter Rule:	200.1.1.0	(Source IP Network Address)
	255.255.255.128	(Source IP Mask)
	Forward = No	(What happens on match)

Incoming packet has the source address of 200.1.1.28

IP Address	Binary Representation	
200.1.1.28	00011100	(Source address in incoming IP packet)
AND		
255.255.255.128	10000000	(Perform the logical AND)
	00000000	(Logical AND result)

This incoming IP packet has a source IP address that matches the network address in the Source IP Address field (00000000) in the Netopia 4753. This will *not* forward this packet.

Example 2

Filter Rule:	200.1.1.0	(Source IP Network Address)
	255.255.255.128	(Source IP Mask)
	Forward = No	(What happens on match)

Incoming packet has the source address of 200.1.1.184.

IP Address	Binary Representation	
200.1.1.184	10111000	(Source address in incoming IP packet)
AND		
255.255.255.128	10000000	(Perform the logical AND)
	10000000	(Logical AND result)

This incoming IP packet (10000000) has a source IP address that does not match the network address in the Source IP Address field (00000000) in the Netopia 4753. This rule *will* forward this packet because the packet does not match.

Example 3

Filter Rule:	200.1.1.96	(Source IP Network Address)
	255.255.255.240	(Source IP Mask)
	Forward = No	(What happens on match)

Incoming packet has the source address of 200.1.1.184.

IP Address	Binary Representation	
200.1.1.184	10111000	(Source address in incoming IP packet)
AND		
255.255.255.240	11110000	(Perform the logical AND)
	10110000	(Logical AND result)

Since the Source IP Network Address in the Netopia 4753 is 01100000, and the source IP address after the logical AND is 1011000, this rule does *not* match and this packet will be forwarded.

Example 4

Filter Rule:	200.1.1.96	(Source IP Network Address)
	255.255.255.240	(Source IP Mask)
	Forward = No	(What happens on match)

Incoming packet has the source address of 200.1.1.104.

IP Address	Binary Representation	
200.1.1.104	01101000	(Source address in incoming IP packet)
AND		
255.255.255.240	11110000	(Perform the logical AND)
	01100000	(Logical AND result)

Since the Source IP Network Address in the Netopia 4753 is 01100000, and the source IP address after the logical AND is 01100000, this rule *does* match and this packet will *not* be forwarded.

Example 5

Filter Rule:	200.1.1.96	(Source IP Network Address)
	255.255.255.255	(Source IP Mask)
	Forward = No	(What happens on match)

Incoming packet has the source address of 200.1.1.96.

IP Address	Binary Representation	
200.1.1.96	01100000	(Source address in incoming IP packet)
AND		
255.255.255.255	11111111	(Perform the logical AND)
	01100000	(Logical AND result)

Since the Source IP Network Address in the Netopia 4753 is 01100000, and the source IP address after the logical AND is 01100000, this rule *does* match and this packet will *not* be forwarded. This rule masks off a *single* IP address.

LAN IP Filtersets

The Netopia 4753 offers LAN-side filtering on the Ethernet hub. This permits multiple IP addresses or subnets on the Ethernet LAN to be kept separate from one another and operate as virtual independent networks sharing a single Internet connection. Small- to medium-sized offices can benefit by using a single router to connect to the Internet, with multiple businesses within the office using independent subnets on the network. Schools can benefit by separating the administrative network from the student network.

A LAN-side filter is the reverse of a WAN-side filter. When you use a WAN-side filter you are restricting external access to your internal network. The most common type of WAN-side filter is the Basic Firewall that is pre-defined in Netopia routers.

When you create a LAN-side filter you are restricting access from your internal network to the external world, or to other subnets on your internal network.

The main advantage of filtering from the LAN is to limit users (or a set of users on a subnet) from accessing services such as telnet to the router to make configuration changes or accessing the Internet via HTTP.

Companies desiring to limit certain departments from accessing the Internet can use LAN-side filtering, as well as schools desiring to prevent their student network from downloading files via FTP etc.

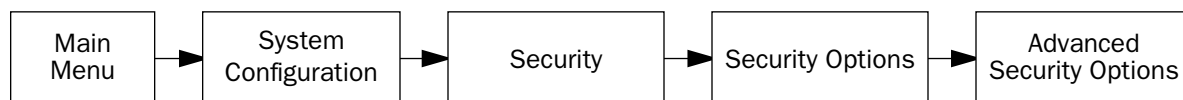
The WAN filtersets Basic Firewall and NetBIOS Filter should never be applied to your internal LAN because they can cut off access from all of your internal computers to the router itself. Instead, you should create separate new filtersets to be applied to the router's Ethernet hub to restrict user and subnet access to other subnets or to the Internet.

Filtersets are very powerful access-restriction tools, and for this reason, the LAN-side filterset binding menu is placed in the Advanced Security Options screen.

Before attempting to create and use LAN-side filtersets, you should read and understand fully the information on subnet and filterset creation. For information on creating multiple subnets, see [Chapter 10, "IP Setup."](#)

After you have created an appropriate filterset, you apply it to the Ethernet hub interface as follows:

To attach a filter set to the Ethernet hub interface, navigate to the **Advanced Security Options** screen from the **Main Menu**.



Any customized filter set you create can be associated with the Ethernet hub as shown below:

Advanced Security Options

Security Databases... Local only

RADIUS Server Addr/Name:
 RADIUS Server Secret:
 Alt RADIUS Server Addr/Name:
 Alt RADIUS Server Secret:
 RADIUS Identifier:
 RADIUS Server Authentication Port: 1812

LAN (EN Hub) IP Filter Set...
 Remove Filter Set

Select **LAN (EN Hub) IP Filter Set** and from the pop-up menu, select the filter set you want to associate with the LAN interface.

Advanced Security Options

Security Databases... Local only

RADIUS Server Addr/Name:
 RADIUS Server Secret:
 Alt RADIUS Server Addr/Name:
 Alt RADIUS Server Secret:
 RADIUS Identifier:-----+
 RADIUS Server Aut+-----+

LAN (EN Hub) IP F
 Remove Filter Set

Basic Firewall
 NetBIOS Filter
 My LAN Filterset 1
 My LAN Filterset 2

Up/Down Arrows to select, then Return/Enter; ESC to cancel.

Press **Return**. The filter set you select will be applied to the Ethernet hub interface.

CAUTION! You should not attach the default filter sets **Basic Firewall** or **NetBIOS Filter** to the Ethernet LAN or its subnets. This may result in a loss of connectivity to the network or subnet. Instead, create a **new** filter set in accordance with the standard filtering rules described earlier.

To remove the filter set from the Ethernet hub interface, select **Remove Filter Set** and press **Return**. The filter set will be disconnected from the LAN interface.

Note: Removing the filter set from the LAN does not delete the filter set. It is still available to be reassociated with the same or another interface, or modified further.

RADIUS Client Support

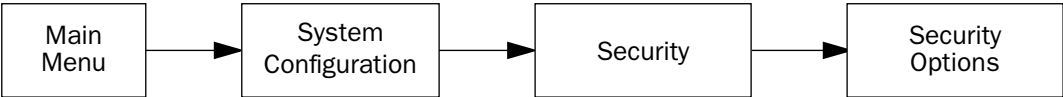
The Netopia 4753 implements a Remote Authentication Dial-In User Service (RADIUS) client (RFC 2138) and adds the ability to authenticate console configuration access using a RADIUS server. This feature is strictly for console menu access authentication only and is not intended for WAN connectivity access authentication.

The Netopia 4753 has the ability to authenticate users seeking console configuration access by using a remote authentication database maintained by a RADIUS server. It supports four security database modes:

- Local Only
- RADIUS only
- RADIUS then Local
- Local then RADIUS

RADIUS client configuration

To display the Security Options screen, from the Main Menu select System Configuration, Security, then Security Options.



Security Options

Enable Dial-in Console Access:

Yes

Enable SmartStart/Web Server:

Yes

Enable Telnet Console Access:

Yes

Enable Telnet Access to SNMP Screens:

Yes

Console Access timeout (seconds):

600

Show Users...

Add User...

Delete User...

Advanced Security Options...

Password for this Screen (11 chars max):

Set up configuration access options here.

If you select **Advanced Security Options** and press Return, the Advanced Security Options screen appears.

Advanced Security Options	
Security Databases...	Local only RADIUS only RADIUS then Local Local then RADIUS
RADIUS Server Addr/Name:	
RADIUS Server Secret:	
Alt RADIUS Server Addr/Name:	
Alt RADIUS Server Secret:	
RADIUS Identifier:	
RADIUS Server Authentication Port: 1812	

- You select your desired mode by using the **Security Databases** pop-up menu.
 - Choosing **Local Only**, the default, selects the local authentication database.
 - Choosing **RADIUS Only** causes the router to ignore the local database and to authenticate users using the configured RADIUS server.
 - Choosing **RADIUS then Local** causes the router to attempt to authenticate a user first using a RADIUS server and then, if that fails, using the local authentication database.
 - Choosing **Local then RADIUS** causes the router to attempt to authenticate a user first using the local authentication database, and then, if that fails using the configured RADIUS server.

Note: In the latter two modes that involve both RADIUS and the local database, if the local database includes no username/password pairs, authentication will succeed only if the RADIUS server authenticates the user. This differs from the Local Only mode where no authentication is performed when the local database is empty.

If the primary RADIUS server responds with an access rejection or an access challenge, the alternate RADIUS server is not contacted. Only if the primary RADIUS server fails to respond at all is the alternate RADIUS server contacted.

Therefore, do not attempt to select any of the RADIUS options unless you have a RADIUS server correctly configured for this purpose. If you attempt to use RADIUS authentication without a RADIUS server, you will lose your configuration access to the router.

The Advanced Security Options screen supports both a primary RADIUS server and an alternate RADIUS server. When the router is configured to authenticate using RADIUS, it will first attempt to contact the primary RADIUS server; if the primary RADIUS server responds, RADIUS authentication succeeds or fails based on the response returned by the primary server. If and only if the primary server fails to respond, the router will attempt to contact the alternate RADIUS server to authenticate the user. The router makes two attempts per server, three seconds apart.

- You can specify the **RADIUS Server Addr/Name** and the **Alt RADIUS Server Addr/Name** either by using a

13-32 Administration Guide

hostname to be resolved using the Domain Name System (DNS) information configured in the router or by using an IP address in dotted-quad notation. The RADIUS Server Addr/Name items are limited to 63 characters.

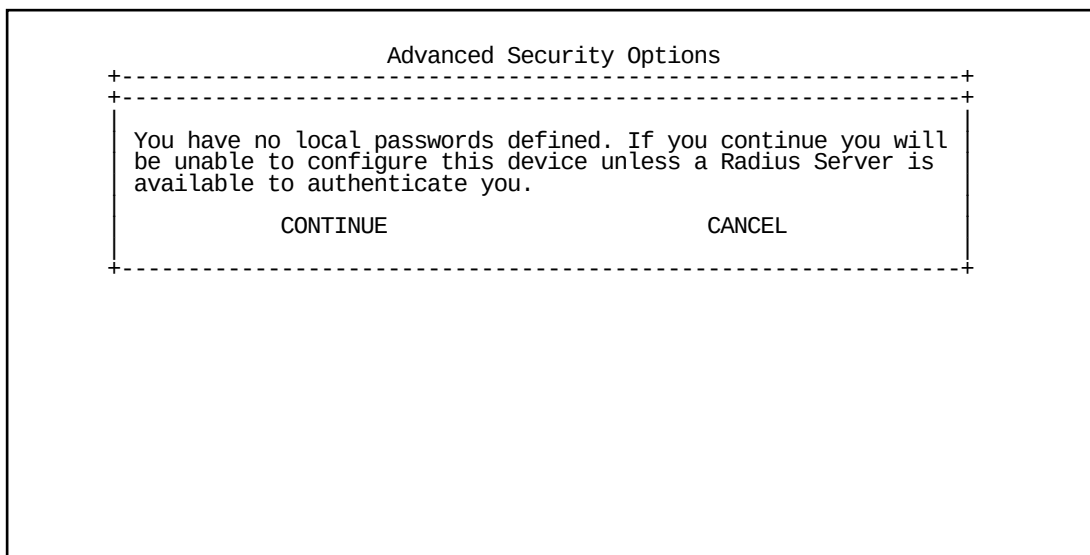
- In addition to specifying the server's hostname or IP address, you must also specify a **RADIUS Server Secret** and an **Alt RADIUS Server Secret** (if configured) known to both the router and the RADIUS server. The secret is used to encrypt RADIUS transactions in transit. The RADIUS Server Secret items are limited to 31 characters.

The router's RADIUS client implementation supports passwords longer than 16 characters and properly encrypts such passwords per RFC 2138. Not all RADIUS server implementations handle passwords longer than 16 characters.

- **RADIUS Identifier** can be either an IP address or an arbitrary string to be used as the identifier in the router's outgoing Access-Request packets. The RADIUS identifier is limited to 63 characters.
- **RADIUS Server Authentication Port** specifies the UDP destination port to which the router's RADIUS authentication requests will be sent. The default value is 1812, the official IANA-assigned UDP port number for the RADIUS authentication service.

Warning alerts

Certain security-related configuration changes cause the router to display a warning alert. Choosing either **Local then RADIUS** or **RADIUS then Local** from the Security Databases pop-up menu when there are no configured username/password pairs causes the router to present the following warning alert:



Attempting to delete the last non-URG username/password pair from the local authentication database when the Security Databases pop-up menu is set to either **Local then RADIUS** or **RADIUS then Local** causes the router to present the following warning alert:

```

                                Security Options
          +-----+
          +-----+
          | You are about to delete the only local password. If you
          | continue you will be unable to configure this device unless
          | a Radius Server is available to authenticate you.
          |
          |          CONTINUE                      CANCEL
          |
          +-----+
          | Show Users...          +-----+
          | Add User...           +-----+
          | Delete User...        | Netopia URG
          |                       | tonyf
          | Advanced Security Optio
          | Password for This Screenshot):
  
```

Note: Any RADIUS server database entry that will be used to authenticate users attempting to gain console access to a Netopia device must specify the Administrative service type (Service-Type 6).

Chapter 14

Monitoring Tools

This chapter discusses the Netopia 4753's device and network monitoring tools. These tools can provide statistical information, report on current network status, record events, and help in diagnosing and locating problems.

This section covers the following topics:

- “Quick View Status Overview” on page 14-1
- “Statistics & Logs” on page 14-4
- “Event Histories” on page 14-4
- “Voice Logs” on page 14-7
- “IP Routing Table” on page 14-9
- “Served IP Addresses” on page 14-10
- “General Statistics” on page 14-11
- “System Information” on page 14-13
- “SNMP” on page 14-13

Quick View Status Overview

You can get a useful, overall status report from the Netopia 4753 in the Quick View screen. To go to the Quick View screen, select **Quick View** in the Main Menu.



The Quick View screen has three status sections:

- General status
- Current WAN Connection Status
- LED Status

The status sections vary according to the interface of your Netopia 4753.

General status

Quick View

1/5/2001 02:41:39 PM

Default IP Gateway: 0.0.0.0

CPU Load: 5%

Unused Memory: 602 KB

Primary DNS Server: 0.0.0.0

Domain Name: netopia.com

Secondary DNS Server: 0.0.0.0

-----MAC Address-----IP Address-----

Ethernet Hub: 00-00-c5-70-03-48 192.168.1.1

ATM g.SHDSL: 00-00-c5-70-03-4a 0.0.0.0

Current DSL Status

Profile Name-----Rate--%Use-Remote Address-----Est.-More Info-----

ISP 1536 10 IP 92.163.4.1 Lcl NAT 192.163.100.6

VPN QuickView

LED Status

-PWR---ERROR---ETHERNET---DSL-----VOICE-----+-----LEDS-----

G - - - - - 1 2 3 4 5 6 7 8 | '-'= Off 'G'= Green

G G G G G G G G | 'R'= Red 'Y'= Yellow

- Current Date:** The current date; this can be set with the Date and Time utility either automatically via NTP or manually (see [“Date and time \(Network Time Protocol\)” on page 9-17](#)).
- Default IP Gateway:** The router’s default gateway, which may be either manually configured or learned via DHCP. This is the value you assigned in the Default IP Gateway field on [page 10-3](#). If you are using the router’s defaults (DHCP and NAT) this value will be 0.0.0.0. If you have assigned an IP address as your default gateway, it is shown here.
- CPU Load:** Percentage of the system’s resources being used by all current transmissions.
- Unused Memory:** The total remaining system memory available for use.
- Primary DNS Server:** If you are using the router’s defaults (DHCP and NAT) this value will be 0.0.0.0. If you have assigned an IP address as your primary domain name server, it is shown here.
- Secondary DNS Server:** If you are using the router’s defaults (DHCP and NAT) this value will be 0.0.0.0. If you have assigned an IP address as a secondary domain name server, it is shown here.
- Domain Name:** The domain name you have assigned, typically the name of your ISP.
- MAC Address:** The Netopia 4753’s hardware address, for those interfaces that support DHCP.
- IP Address:** The Netopia 4753’s IP address, entered in the IP Setup screen.

Current status

The current status section is a table showing the current status of the WAN. For example:

Current DSL Status					
Profile Name-----	Rate--	%Use-	Remote Address----	Est.-	More Info-----
ISP	1536	10	IP 92.163.4.1	Lcl	NAT 192.163.100.6

- Profile Name:** Lists the name of the connection profile being used, if any.
- Rate:** Shows the line rate for this connection.
- %Use:** Indicates the average percent utilization of the maximum capacity of the channels in use for the connection.
- Remote Address:** Shows the IP address of the connected remote router if the connection is using IP.
- Est:** Indicates whether the connection was locally (“Lcl”) or remotely (“Rmt”) established.
- More Info:** Indicates, in order of priority, the NAT address in use for this connection or the caller identification (if available).

Status lights

This section shows the current real-time status of the Netopia 4753’s status lights (LEDs). It is useful for remotely monitoring the router’s status. The Quick View screen’s arrangement of LEDs corresponds to the physical arrangement of LEDs on the router. The active voice ports are also indicated.

LED Status															
-PWR----	ERROR----	ETHERNET----	DSL-----	-VOICE-----								+	-----LEDS-----		
G	-	-	-	-	1	2	3	4	5	6	7	8		'-'= Off	'G'= Green
					G	G						G		'R'= Red	'Y'= Yellow

- Each LED representation can report one of four states:
- : The LED is off.
 - R:** The LED is red.
 - G:** The LED is green.
 - Y:** The LED is yellow.
- The section “[Netopia 4753 Status Lights](#)” on page 3-5 describes the meanings of the colors for each LED.

Statistics & Logs



When you are troubleshooting your Netopia 4753, the Statistics & Logs screens provide insight into the recent event activities of the router.

From the Main Menu go to Statistics & Logs and select one of the options described in the sections below.

Event Histories

The Netopia 4753 records certain relevant occurrences in event histories. Event histories are useful for diagnosing problems because they list what happened before, during, and after a problem occurs. You can view two different event histories: one for the router’s system and one for the WAN. The Netopia 4753’s built-in battery backup prevents loss of event history from a shutdown or reset.

The router’s event histories are structured to display the most recent events first, and to make it easy to distinguish error messages from informational messages. Error messages are prefixed with an asterisk. Both the WAN Event History and Device Event History retain records of the 128 most recent events.

In the Statistics & Logs screen, select **WAN Event History**. The WAN Event History screen appears.



WAN Event History

The WAN Event History screen lists a total of 128 events on the WAN. The most recent events appear at the top.

```

                                WAN Event History
                                Current Date -- 12/3/98 03:02:23 PM
-Date-----Time-----Event-----
-----SCROLL UP-----
07/03/98 13:59:06   DSL: IP up, channel 1, gateway: 173.166.107.1
07/03/98 13:59:05   DSL: Channel 1 up
07/03/98 13:59:05 >>WAN: data link activated at 1040 Kbps
07/03/98 13:58:32   --Device restarted-----
07/03/98 12:46:39   --Device restarted-----
07/03/98 11:45:57   --Device restarted-----
07/02/98 17:58:15   DSL: IP up, channel 1, gateway: 173.166.107.1
07/02/98 17:58:10   DSL: Channel 1 up
07/02/98 17:58:10 >>WAN: data link activated at 1040 Kbps
07/02/98 17:57:05   DSL: IP down, channel 1
07/02/98 17:57:05   Link 1 down: No Synch
07/02/98 17:57:05 >>WAN: data link deactivated
07/02/98 17:48:02   DSL: IP up, channel 1, gateway: 173.166.107.1
07/02/98 17:48:01   DSL: Channel 1 up
-----SCROLL DOWN-----
Clear History...

Return/Enter on event item for details or SCROLL [UP/DOWN] item for scrolling.
```

Each entry in the list contains the following information:

- Date:** Date of the event.
 - Time:** Time of the event.
 - Event:** A brief description of the event.
 - Ch.:** The channel involved in the event.
 - Dir. Number:** The directory number (number dialed) involved in the event (switched circuit models only).
- The first event in each call sequence is marked with double arrows (>>).
- Failures are marked with an asterisk (*).
- If the event history exceeds the size of the screen, you can scroll through it by using the SCROLL UP and SCROLL DOWN items.
- To scroll up, select **SCROLL UP** at the top of the list and press Return. To scroll down, select **SCROLL DOWN** at the bottom of the list and press Return.
- To get more information about any event listed in the WAN Event History, select the event and then press Return. A dialog box containing more information about the selected event will appear. Press Return or Escape to dismiss the dialog box.
- To clear the event history, select **Clear History** at the bottom of the history screen and press Return.

Device Event History

The Device Event History screen lists a total of 128 port and system events, giving the time and date for each event, as well as a brief description. The most recent events appear at the top.

In the Statistics & Logs screen, select **Device Event History**. The Device Event History screen appears.

```

                                Device Event History
                                Current Date -- 1/18/01 10:34:14 AM
-Date-----Time-----Event-----
-----SCROLL UP-----
01/18/01 08:25:42   IP address server initialization complete
01/18/01 08:25:40 --BOOT: Cold start v5.0 -----
01/17/01 11:21:13   IP address server initialization complete
01/17/01 11:21:11 --BOOT: Warm start v5.0 -----
01/17/01 11:21:00   CONSOLE: Reverted to default configuration

-----SCROLL DOWN-----
Clear History...

Return/Enter on event item for details or SCROLL [UP/DOWN] item for scrolling.
```

If the event history exceeds the size of the screen, you can scroll through it by using SCROLL UP and SCROLL DOWN.

To scroll up, select **SCROLL UP** at the top of the list and press Return. To scroll down, select **SCROLL DOWN** at the bottom of the list and press Return.

To obtain more information about any event listed in the Device Event History, select the event and then press Return. A dialog box containing more information about the selected event appears. Press Return or Escape to dismiss the dialog box.

To clear the Device Event History, select **Clear History** and press Return.

Voice Logs

Voice Log

The Voice Log screen lists a total of 128 voice-related events, giving the time and date for each event, as well as a brief description. The most recent events appear at the top.

In the Statistics & Logs screen, select **Voice Log**. The Voice Log screen appears.

Voice Log			
		Current Date --	1/5/01 06:00:45 AM
-Date-----	Time-----	Event-----	
-----SCROLL UP-----			
01/05/01	11:03:27	Voice gateway link yes.	IP: 163.176.232.4
01/05/01	05:26:23	Voice gateway link yes.	IP: 163.176.232.4
01/05/01	12:02:41	Voice gateway link no.	
01/05/01	12:02:31	Voice gateway link yes.	IP: 163.176.232.4
01/05/01	11:52:25	Voice gateway link yes.	IP: 163.176.232.4
01/05/01	11:49:23	Voice gateway link yes.	IP: 163.176.232.4
01/05/01	11:46:26	Voice gateway link yes.	IP: 163.176.232.4
01/05/01	11:44:39	Voice gateway provisioned for TOLLBRIDGE	
-----SCROLL DOWN-----			
Clear History...			

If the log exceeds the size of the screen, you can scroll through it by using SCROLL UP and SCROLL DOWN.

To scroll up, select **SCROLL UP** at the top of the list and press Return. To scroll down, select **SCROLL DOWN** at the bottom of the list and press Return.

To obtain more information about any event listed in the Voice Log, select the event and then press Return. A dialog box containing more information about the selected event appears. Press Return or Escape to dismiss the dialog box.

To clear the Voice Log, select **Clear History** and press Return.

Voice Accounting Log

The Voice Accounting Log screen lists a total of 128 voice-related events, giving the time and date for each event, as well as a brief description. The most recent events appear at the top.

In the Statistics & Logs screen, select **Voice Accounting Log**. The Voice Accounting Log screen appears.

```

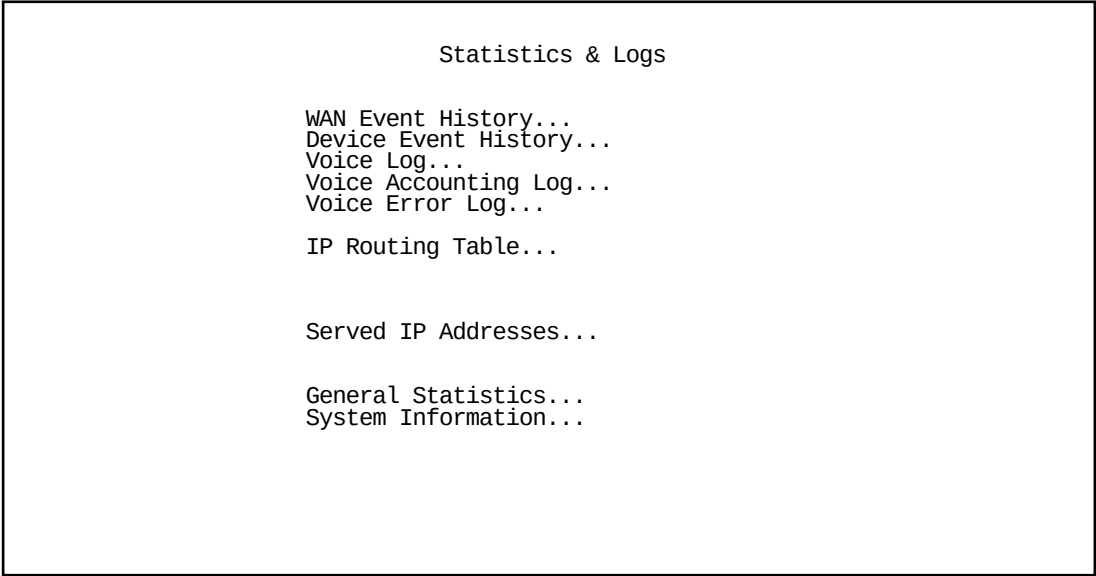
Voice Accounting Log
Current Date -- 1/5/01 01:46:27 PM
-Date-----Time-----Event-----
-----SCROLL UP-----
1/5/01 05:29:08 Out 231 to 333 Duration: 00:00:14
1/5/01 05:28:53 Out 226 to 511 Duration: 00:00:01
1/5/01 05:28:49 Out 446 to 444 Duration: 00:00:10
-----SCROLL DOWN-----
Clear History...

```

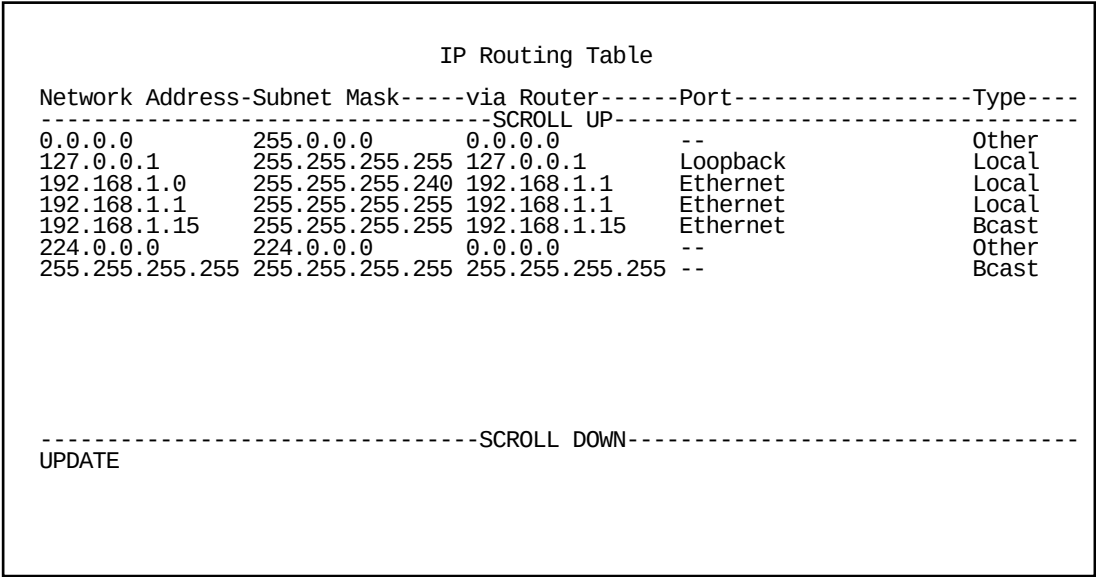
- If the log exceeds the size of the screen, you can scroll through it by using SCROLL UP and SCROLL DOWN.
- To scroll up, select **SCROLL UP** at the top of the list and press Return. To scroll down, select **SCROLL DOWN** at the bottom of the list and press Return.
- To obtain more information about any event listed in the Voice Accounting Log, select the event and then press Return. A dialog box containing more information about the selected event appears. Press Return or Escape to dismiss the dialog box.
- To clear the Voice Accounting Log, select **Clear History** and press Return.

IP Routing Table

In the Statistics & Logs screen, select **IP Routing Table** and press Return.



The IP routing table displays all of the IP routes currently known to the Netopia 4753.



The routing table screen represents a snapshot of the routing table information at the time the screen is first invoked. To take a new snapshot, select **Update** at the bottom of the screen and press Return.

Served IP Addresses

You can view all of the IP addresses currently being served by the Netopia 4753 G.SHDSL Integrated Access Device from the **Served IP Addresses** screen.

From the Statistics & Logs menu, select **Served IP Addresses**. The Served IP Addresses screen appears.

Served IP Addresses			
-IP Address-----	Type----	Expires----	Client Identifier-----
-----SCROLL UP-----			
192.168.1.100	DHCP	00:36	EN: 00-00-c5-4a-1f-ea
192.168.1.101	DHCP	00:58	EN: 08-00-07-16-0c-85
192.168.1.102			
192.168.1.103			
192.168.1.104			
192.168.1.105			
192.168.1.106			
192.168.1.107			
192.168.1.108			
192.168.1.109			
192.168.1.110			
192.168.1.111			
192.168.1.112			
192.168.1.113			
-----SCROLL DOWN-----			
Lease Management...			

To manage DHCP leases, select **Lease Management** in this screen.

The IP Address Lease Management screen appears.

IP Address Lease Management	
Reset All Leases	
Release BootP Leases	
Reclaim Declined Addresses	
Hit RETURN/ENTER, you will return to the previous screen.	

This screen has three options:

- **Reset All Leases:** Resets all current IP addresses leased through DHCP without waiting for the default one-hour lease period to elapse
- **Release BootP Leases:** Releases any BootP leases that may be in place and which may no longer be required.
- **Reclaim Declined Addresses:** Reclaims served leases that have been declined; for example, by devices that may no longer be on the network.

General Statistics

To go to the General Statistics screen, select **General Statistics** and press Return. The General Statistics screen appears.

General Statistics						
Phys I/F-----	Rx Bytes---	Tx Bytes---	Rx Pkts---	Tx Pkts---	Rx Err----	Tx Err----
Ethernet Hub	123456789	123456789	12345678	12345678	12345678	12345678
SDSL 1	123456789	123456789	12345678	12345678		
Network-----	Rx Bytes---	Tx Bytes---	Rx Pkts---	Tx Pkts---	Rx Err----	Tx Err----
IP	123456789	123456789	12345678	12345678	12345678	12345678

The General Statistics screen displays information about data traffic on the Netopia 4753’s data ports. This information is useful for monitoring and troubleshooting your LAN. Note that the counters roll over at their maximum field width, that is, they restart again at 0.

Physical Interface

The top left side of the screen lists total packets received and total packets transmitted for the following data ports:

- Ethernet Hub
- SDSL 1

Network Interface

The bottom left side of the screen lists total packets received and total packets transmitted for the following protocols:

- IP (IP packets on the Ethernet)

The right side of the table lists the total number of occurrences of each of six types of communication statistics:

- Rx Bytes:** The number of bytes received
- Tx Bytes:** The number of bytes transmitted
- Rx Packets:** The number of packets received
- Tx Pkts:** The number of packets transmitted
- Rx Err:** The number of bad Ethernet packets received
- Tx Err:** The number of errors occurring when Ethernet packets are transmitted simultaneously by nodes on the LAN

System Information

The System Information screen gives a summary view of the general system level values in the Netopia 4753 G.SHDSL Integrated Access Device.

From the Statistics & Logs menu select **System Information**. The System Information screen appears.

System Information	
Serial Number	ff-70-00 (16740352)
Firmware Version	5.0
Processor Speed (MHz)	50
Flash ROM Capacity (MBytes)	2
DRAM Capacity (MBytes)	16
Ethernet	Single 10/100 Port
WAN Interface	ATM SDSL

The information display varies by model, firmware version, feature set, and so on. You can tell at a glance your particular system configuration.

SNMP

The Netopia 4753 includes a Simple Network Management Protocol (SNMP) agent, allowing monitoring and configuration of many of the data routing features by a standard SNMP manager.

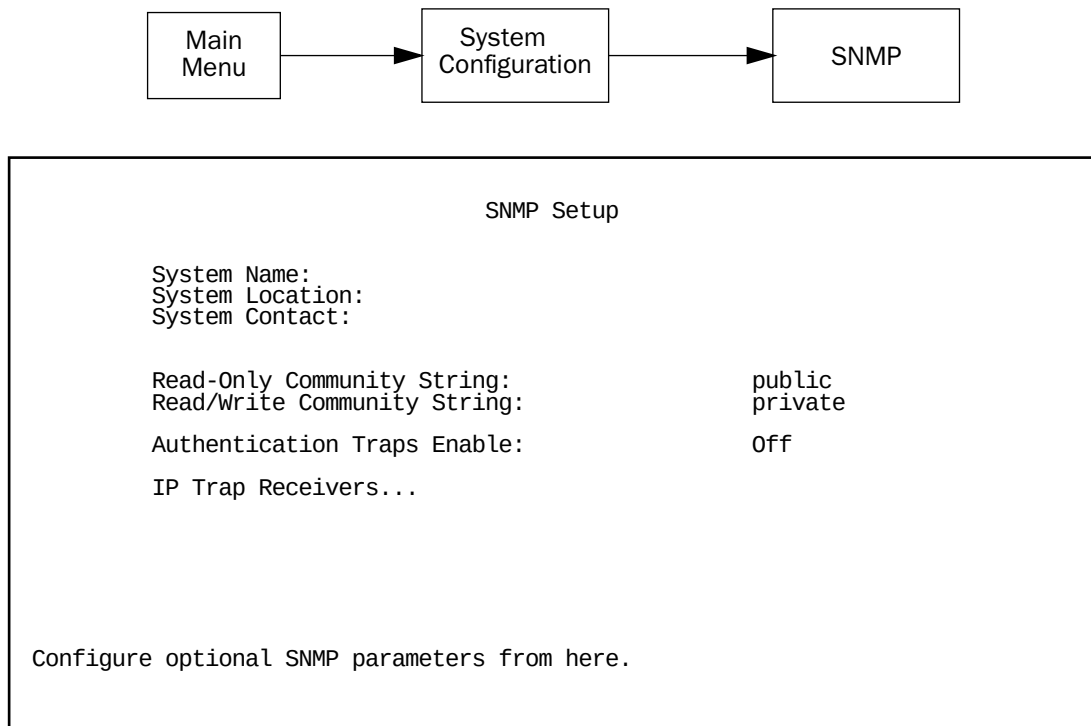
The Netopia 4753 supports the following management information base (MIB) documents:

- MIB II (RFC 1213)
- Interface MIB (RFC 1229)
- Ethernet MIB (RFC 1643)
- Netopia MIB

These MIBs are on the Netopia 4753 CD included with the Netopia 4753. Load these MIBs into your SNMP management software in the order they are listed here. Follow the instructions included with your SNMP manager on how to load MIBs.

The SNMP Setup screen

From the Main Menu, select **SNMP** in the System Configuration screen and press Return. The SNMP Setup screen appears.



Follow these steps to configure the first three items in the screen:

1. Select **System Name** and enter a descriptive name for the Netopia 4753's SNMP agent.
2. Select **System Location** and enter the router's physical location (room, floor, building, etc.).
3. Select **System Contact** and enter the name of the person responsible for maintaining the router.

System Name, System Location, and System Contact set the values returned by the Netopia 4753 SNMP agent for the SysName, SysLocation, and SysContact objects, respectively, in the MIB II system group. Although optional, the information you enter in these items can help a system administrator manage the network more efficiently.

Community strings

The **Read-Only Community String** and the **Read/Write Community String** are like passwords that must be used by an SNMP manager querying or configuring the Netopia 4753. An SNMP manager using the **Read-Only Community String** can examine statistics and configuration information from the router, but cannot modify the router's configuration. An SNMP manager using the **Read/Write Community String** can both examine and modify configuration parameters.

By default, the read-only and read/write community strings are set to public and private, respectively. You should change both of the default community strings to values known only to you and trusted system administrators.

To change a community string, select it and enter a new value.

Starting with the version 4.3 firmware, setting the Read-Only and Read-Write community strings to the empty string will block all SNMP requests to the router. (The router may still send SNMP Traps if those are properly enabled.)

Previously, if either community string was the empty string, SNMP Requests specifying an empty community string were accepted and processed.

This change is designed to allow the administrator to block SNMP access to the router and to provide more granular control over the allowed SNMP operations to the router.

- Setting only the Read-Write community string to the empty string will block SNMP Set Requests to the router, but Get Requests and Get-Next Requests will still be honored using the Read-Only community string (assuming that is not the empty string).
- Setting only the Read-Only community string to the empty string will *not* block Get Requests or Get-Next Requests since those operations (and Set Requests) are still allowed using the (non-empty) Read-Write community string.

Even if you decide not to use SNMP, you should change the community strings. This prevents unauthorized access to the Netopia 4753 through SNMP. For more information on security issues, see [“Suggested Security Measures” on page 13-1](#).

SNMP traps

An SNMP trap is an informational message sent from an SNMP agent (in this case, the Netopia 4753) to a manager. When a manager receives a trap, it may log the trap as well as generate an alert message of its own.

Standard traps generated by the Netopia 4753 include the following:

- An authentication failure trap is generated when the router detects an incorrect community string in a received SNMP packet. **Authentication Traps Enable** must be **On** for this trap to be generated.
- A cold start trap is generated after the router is reset.
- An interface down trap (ifDown) is generated when one of the router’s interfaces, such as a port, stops functioning or is disabled.
- An interface up trap (ifUp) is generated when one of the router’s interfaces, such as a port, begins functioning.

The Netopia 4753 sends traps using UDP (for IP networks).

You can specify which SNMP managers are sent the IP traps generated by the Netopia 4753. Up to eight receivers can be set. You can also review and remove IP traps.

To go to the IP Trap Receivers screen, select **IP Trap Receivers**. The IP Trap Receivers screen appears.

IP Trap Receivers

Display/Change IP Trap Receiver...

Add IP Trap Receiver...

Delete IP Trap Receiver...

Return/Enter to modify an existing Trap Receiver.
Navigate from here to view, add, modify and delete IP Trap Receivers.

Setting the IP trap receivers

1. Select **Add IP Trap Receiver**.
2. Select **Receiver IP Address or Domain Name**. Enter the IP address or domain name of the SNMP manager you want to receive the trap.
3. Select **Community String** if you enabled one in the SNMP Setup screen, and enter the appropriate password.
4. Select **Add Trap Receiver Now** and press Return. You can add up to seven more receivers.

Viewing IP trap receivers

To display a view-only table of IP trap receivers, select **Display/Change IP Trap Receiver** in the IP Trap Receivers screen.

Modifying IP trap receivers

1. To edit an IP trap receiver, select **Display/Change IP Trap Receiver** in the IP Trap Receivers screen.
2. Select an IP trap receiver from the table and press Return.
3. In the **Change IP Trap Receiver** screen, edit the information as needed and press Return.

Deleting IP trap receivers

1. To delete an IP trap receiver, select **Delete IP Trap Receiver** in the IP Trap Receivers screen.
2. Select an IP trap receiver from the table and press Return.
3. In the dialog box, select **Continue** and press Return.

Chapter 15

Utilities and Diagnostics

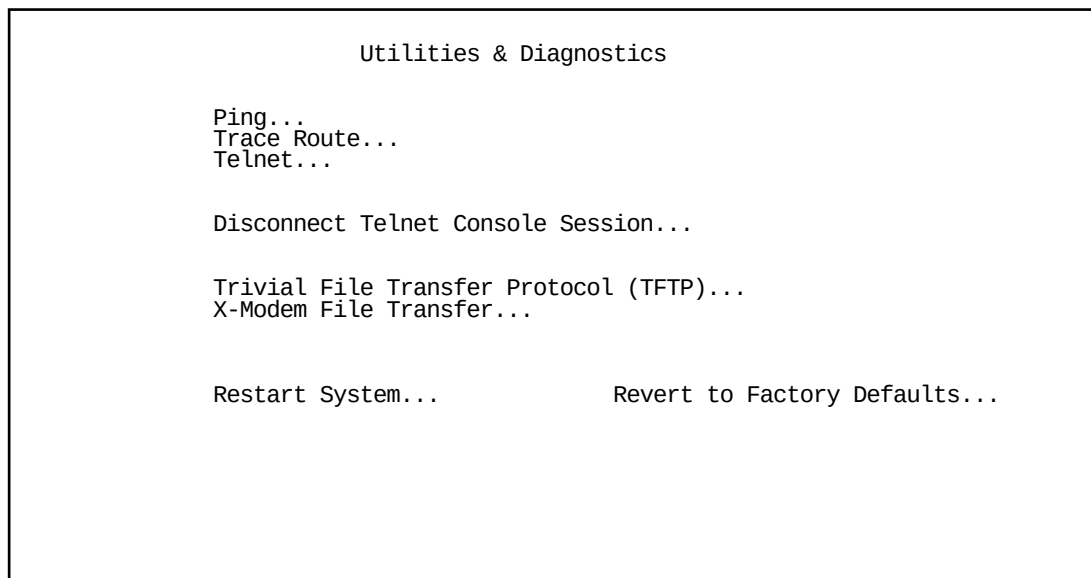
A number of utilities and tests are available for system diagnostic and control purposes.

This section covers the following topics:

- “Ping” on page 15-2
- “Trace Route” on page 15-4
- “Telnet Client” on page 15-5
- “Disconnect Telnet Console Session” on page 15-6
- “Factory Defaults” on page 15-6
- “Transferring Configuration and Firmware Files with TFTP” on page 15-7
- “Transferring Configuration and Firmware Files with XMODEM” on page 15-10
- “Restarting the System” on page 15-12

Note: These utilities and tests are accessible only through the console-based management screens. See [Chapter 6, “Console-Based Management,”](#) for information on accessing the console-based management screens.

You access the Utilities & Diagnostics screens from the Main Menu.



Ping

The Netopia 4753 includes a standard Ping test utility. A Ping test generates IP packets destined for a particular (Ping-capable) IP host. Each time the target host receives a Ping packet, it returns a packet to the original sender.

Ping allows you to see whether a particular IP destination is reachable from the Netopia 4753. You can also ascertain the quality and reliability of the connection to the desired destination by studying the Ping test's statistics.

In the Utilities & Diagnostic screen, select **Ping** and press Return. The ICMP Ping screen appears.

ICMP Ping

Name of Host to Ping:

Packets to Send:

Data Size:

Delay (seconds):

5

56

1

START PING

Status:

Packets Out:

Packets In:

Packets Lost:

Round Trip Time
(Min/Max/Avg):

0

0

0 (0%)

0.000 / 0.000 / 0.000 secs

Enter the IP Address/Domain Name of a host to ping.
Send ICMP Echo Requests to a network host.

To configure and initiate a Ping test, follow these steps:

1. Select **Name of Host to Ping** and enter the destination domain name or IP address.
2. Select **Packets to Send** to change the default setting. This is the total number of packets to be sent during the Ping test. The default setting is adequate in most cases, but you can change it to any value from 1 to 4,294,967,295.
3. Select **Data Size** to change the default setting. This is the size, in bytes, of each Ping packet sent. The default setting is adequate in most cases, but you can change it to any value from 0 (only header data) to 1664.
4. Select **Delay (seconds)** to change the default setting. The delay, in seconds, determines the time between Ping packets sent. The default setting is adequate in most cases, but you can change it to any value from 0 to 4,294,967. A delay of 0 seconds forces packets to be sent immediately, one after another.
5. Select **START PING** and press Return to begin the Ping test. While the test is running, the **START PING** item becomes **STOP PING**. To manually stop the Ping test, select **STOP PING** and press Return or Escape.

While the Ping test is running and when it is over, a status field and a number of statistical items are active on the screen. These are described below.

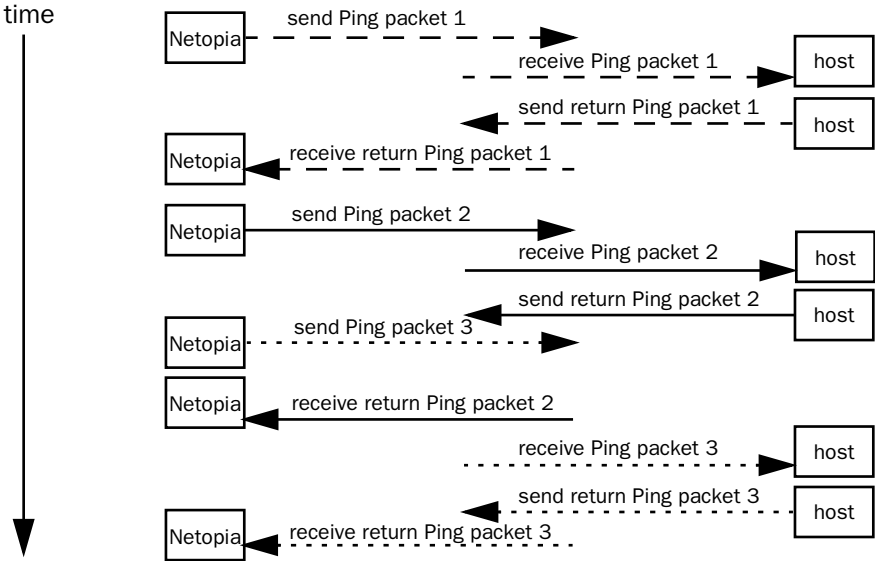
Status: The current status of the Ping test. This item can display the status messages shown in the table below:

Message	Description
Resolving host name	Finding the IP address for the domain name-style address
Can't resolve host name	IP address can't be found for the domain name-style address
Pinging	Ping test is in progress
Complete	Ping test was completed
Cancelled by user	Ping test was cancelled manually
Destination unreachable from w.x.y.z	Ping test was able to reach the router with IP address w.x.y.z, which reported that the test could not reach the final destination
Couldn't allocate packet buffer	Couldn't proceed with Ping test; try again or reset system
Couldn't open ICMP port	Couldn't proceed with Ping test; try again or reset system

Packets Out: The number of packets sent by the Ping test.

Packets In: The number of return packets received from the target host. To be considered on time, return packets are expected back before the next packet in the sequence of Ping packets is sent. A count of the number of late packets appears in parentheses to the right of the **Packets In** count.

In the example that follows, a Netopia 4753 is sending Ping packets to another host, which responds with return Ping packets. Note that the second return Ping packet is considered to be late because it is not received by the Netopia 4753 before the third Ping packet is sent. The first and third return Ping packets are on time.



Packets Lost: The number of packets unaccounted for, shown in total and as a percentage of total packets sent. This statistic may be updated during the Ping test, and may not be accurate until after the test is over. However, if an escalating one-to-one correspondence is seen between **Packets Out** and **Packets Lost**, and **Packets In** is noticeably lagging behind **Packets Out**, the destination is probably unreachable. In this case, use **STOP PING**.

Round Trip Time (Min/Max/Avg): Statistics showing the minimum, maximum, and average number of seconds elapsing between the time each Ping packet was sent and the time its corresponding return Ping packet was received.

The time-to-live (TTL) value for each Ping packet sent by the Netopia 4753 is 255, the maximum allowed. The TTL value defines the number of IP routers that the packet can traverse. Ping packets that reach their TTL value are dropped, and a “destination unreachable” notification is returned to the sender (see the table on the previous page). This ensures that no infinite routing loops occur. The TTL value can be set and retrieved using the SNMP MIB-II ip group’s ipDefaultTTL object.

Trace Route

You can count the number of routers between your Netopia Router and a given destination with the Trace Route utility.

In the Statistics & Diagnostics screen, select **Trace Route** and press Return. The Trace Route screen appears.

Trace Route

Host Name or IP Address:

Maximum Hops:30

Timeout (seconds):5

Use Reverse DNS:Yes

START TRACE ROUTE

Enter the IP Address/Domain Name of a host.
Trace route to a network host.

To trace a route, follow these steps:

1. Select **Host Name or IP Address** and enter the name or address of the destination you want to trace.
2. Select **Maximum Hops** to set the maximum number of routers to count between the Netopia Router and the destination router, up to the maximum of 64. The default is 30 hops.
3. Select **Timeout (seconds)** to set when the trace will timeout for each hop, up to 10 seconds. The default is 3 seconds.

4. Select **Use Reverse DNS** to learn the names of the routers between the Netopia Router and the destination router. The default is Yes.
5. Select **START TRACE ROUTE** and press Return. A scrolling screen will appear that lists the destination, number of hops, IP addresses of each hop, and DNS names, if selected.
6. Cancel the trace by pressing Escape. Return to the Trace Route screen by pressing Escape twice.

Telnet Client

The Telnet client mode replaces the normal menu mode. Telnet sessions can be cascaded, that is, you can initiate a Telnet client session when using a Telnet console session. To activate the Telnet client, select **Telnet** from the Utilities & Diagnostics menu.

The Telnet client screen appears.

Telnet

Host Name or IP Address:

Control Character to Suspend: Q

START A TELNET SESSION

Enter the IP Address/Domain Name of a host.

- Enter the host name or the IP address in dotted decimal format of the machine you want to Telnet into and press Return.
- Either accept the default control character “Q” used to suspend the Telnet session, or type a different one.
- **START A TELNET SESSION** becomes highlighted.
- Press Return and the Telnet session will be initiated.
- To suspend the session, press Control-Q or whatever other control character you specified.

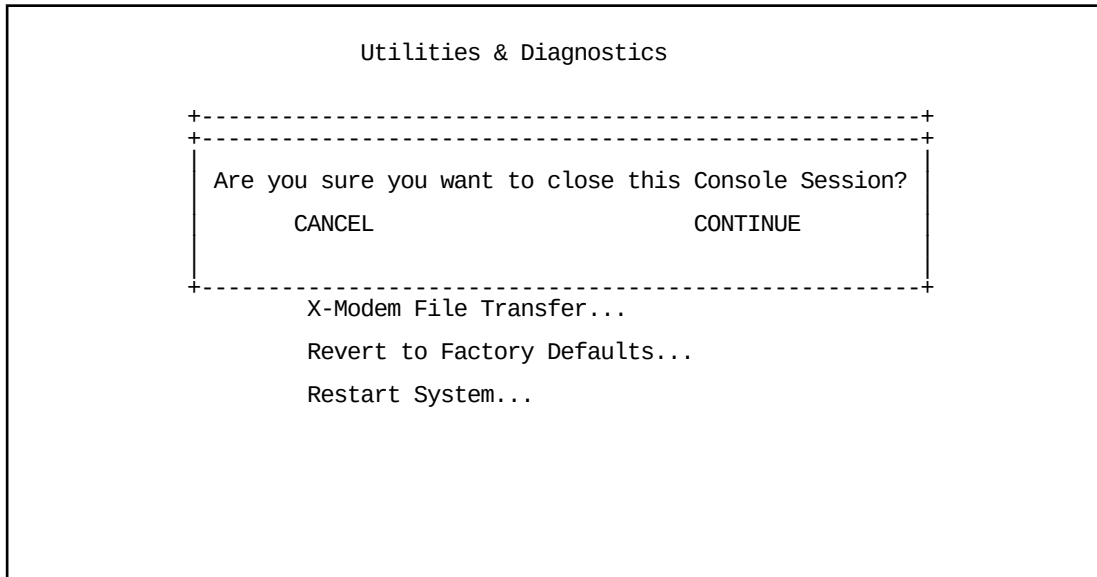
Two new options will appear in the Telnet screen (not shown):

Resume Suspended Session – select if you want to go back to your Telnet session

Terminate Suspended Session – select if you want to end the session

Disconnect Telnet Console Session

If you want to close your Telnet console session, select **Disconnect Telnet Console Session** and press Return. A dialog box appears asking you to cancel or continue your selection.



If you select **Continue**, you will immediately terminate your session.

Factory Defaults

You can reset the Netopia 4753 to its factory default settings. In the Utilities & Diagnostics screen, select **Revert to Factory Defaults** and press Return. Select **CONTINUE** in the dialog box and press Return. The Netopia 4753 will reboot and its settings will return to the factory defaults, deleting your configurations.

In an emergency, you can also use the Reset switch to return the router to its factory default settings. Call Netopia Technical Support for instructions on using the Reset switch.

Note: Reset to factory defaults with caution. You will need to reconfigure all of your settings in the router.

If you lose your password and are unable to access the console screens, you can manually reset the router in an emergency. See [Appendix A, "Troubleshooting."](#)

Transferring Configuration and Firmware Files with TFTP

Trivial File Transfer Protocol (TFTP) is a method of transferring data over an IP network. TFTP is a client-server application, with the router as the client. To use the Netopia 4753 as a TFTP client, a TFTP server must be available. Netopia, Inc., has a public access TFTP server on the Internet where you can obtain the latest firmware versions.

To use TFTP, select **Trivial File Transfer Protocol (TFTP)** in the Statistics & Diagnostics screen and press Return. The Trivial File Transfer Protocol (TFTP) screen appears.

Trivial File Transfer Protocol (TFTP)

TFTP Server Name:
Firmware File Name:
GET ROUTER FIRMWARE FROM SERVER...

Config File Name:
GET CONFIG FROM SERVER...
SEND CONFIG TO SERVER...

TFTP Transfer State -- Idle
TFTP Current Transfer Bytes -- 0

The sections below describe how to update the Netopia 4753's firmware and how to download and upload configuration files.

Updating firmware

Firmware updates may be available periodically from Netopia or from a site maintained by your organization's network administrator.

The Netopia 4753 G.SHDSL Integrated Access Device ships with an embedded operating system referred to as firmware. The firmware governs how the device communicates with your network and the WAN or remote site. Firmware updates are periodically posted on the Netopia website.

To update either the device's firmware, follow these steps:

- Select **TFTP Server Name** and enter the server name or IP address of the TFTP server you will use. The server name or IP address is available from the site where the server is located.
- Select **Firmware File Name** and enter the name of the file you will download. The name of the file is available from the site where the server is located. You may need to enter a file path along with the file name (for example, bigroot/config/myfile).

- Select **GET ROUTER FIRMWARE FROM SERVER** and press Return. You will see the following dialog box:

Are you sure you want to read the firmware now?
The device will reset when the transfer is complete.

CANCEL CONTINUE

- Select **CANCEL** to exit without downloading the file, or select **CONTINUE** to download the file. The system will reset at the end of the file transfer to put the new firmware into effect. While the system resets, the LEDs will blink on and off.

CAUTION! Be sure the firmware update you load onto your router is the correct version for your particular model. Some models do not support all firmware versions. Loading an incorrect firmware version can permanently damage the unit.

Do not manually power down or reset the Netopia 4753 while it is automatically resetting or it could be damaged.

If you choose to download the firmware, the **TFTP Transfer State** item will change from **Idle** to **Reading Firmware**. The **TFTP Current Transfer Bytes** item will reflect the number of bytes transferred.

Downloading configuration files

The Netopia 4753 can be configured by downloading a configuration file using TFTP. Once downloaded, the file reconfigures all of the router's parameters as if someone had manually done so through the console port.

To download a configuration file, follow these steps:

- Select **TFTP Server Name** and enter the server name or IP address of the TFTP server you will use. The server name or IP address is available from the site where the server is located.
- Select **Config File Name** and enter the name of the file you will download. The name of the file is available from the site where the server is located. You may need to enter a file path along with the file name (for example, bigroot/config/myfile).

- Select **GET CONFIG FROM SERVER** and press Return. You will see the following dialog box:

+-----+

+-----+

Are you sure you want to read the configuration now?
The device will reset when the transfer is complete.

CANCEL CONTINUE

+-----+

- Select **CANCEL** to exit without downloading the file, or select **CONTINUE** to download the file. The system will reset at the end of the file transfer to put the new configuration into effect.
- If you choose to download the configuration file, the **TFTP Transfer State** item will change from **Idle** to **Reading Config**. The **TFTP Current Transfer Bytes** item will reflect the number of bytes transferred.

Uploading configuration files

Using TFTP, you can send a file containing a snapshot of the router's current configuration to a TFTP server. The file can then be downloaded by a different Netopia 4753 unit to configure its parameters (see ["Downloading configuration files" on page 15-8](#)). This is useful for configuring a number of routers with identical parameters or just for creating configuration backup files.

Uploading a file can also be useful for troubleshooting purposes. The uploaded configuration file can be tested on a different Netopia 4753 unit by Netopia or your network administrator.

To upload a configuration file, follow these steps:

1. Select **TFTP Server Name** and enter the server name or IP address of the TFTP server you will use. The server name or IP address is available from the site where the server is located.
2. Select **Config File Name** and enter a name for the file you will upload. The file will appear with the name you choose on the TFTP server. You may need to enter a file path along with the file name (for example, Mypc/Netopia/myfile).
3. Select **SEND CONFIG TO SERVER** and press Return. Netopia will begin to transfer the file.
4. The **TFTP Transfer State** item will change from **Idle** to **Writing Config**. The **TFTP Current Transfer Bytes** item will reflect the number of bytes transferred.

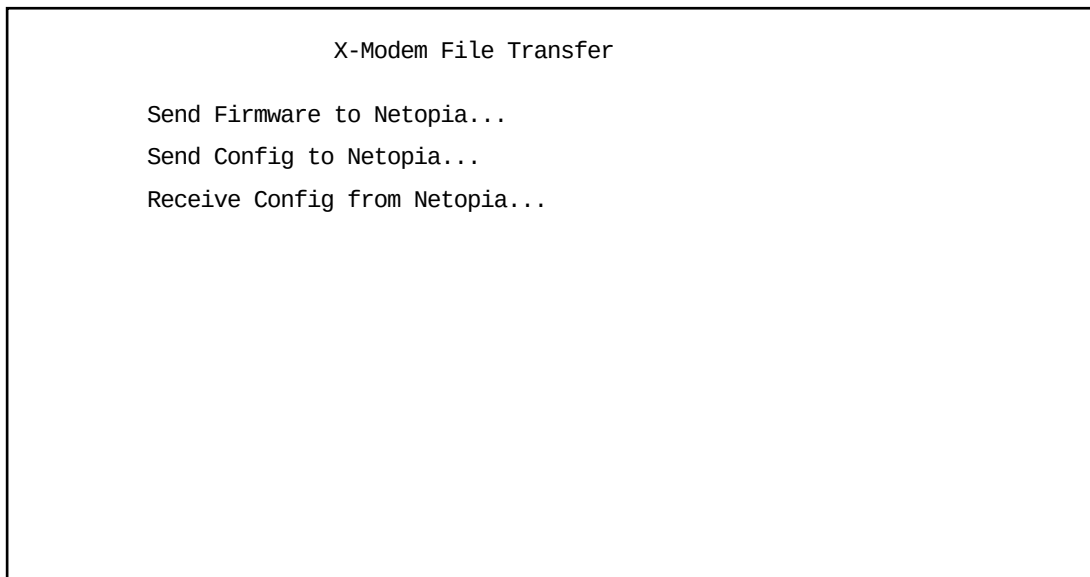
Transferring Configuration and Firmware Files with XMODEM

You can transfer configuration and firmware files with XMODEM through the Netopia 4753's console port. Be sure your terminal emulation program supports XMODEM file transfers.

To go to the **X-Modem File Transfer** screen, select it in the Utilities & Diagnostics menu.

Note: The X-Modem File Transfer screen is only available if you are connected via the Console port.

It is good practice when updating programmable devices to disable any other programs or network activity on the device or the attached computer. This includes WAN traffic such as a DSL connection or screen savers or other automatic programs running on the attached computer. Such activity can slow down or interrupt the file transfer requiring you to rerun the upgrade.

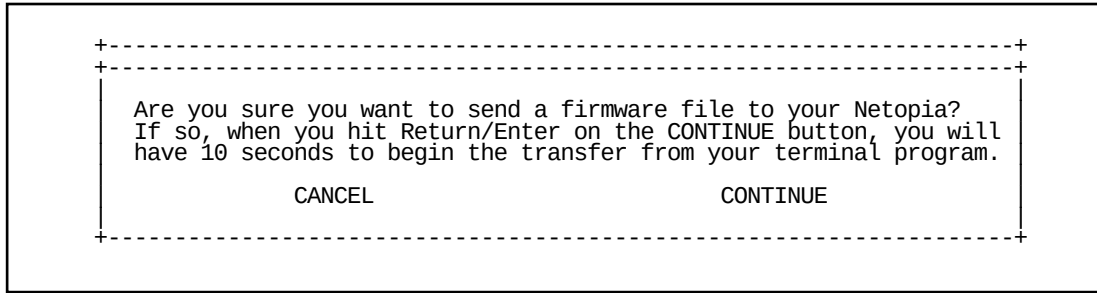


Updating firmware

Firmware updates may be available periodically from Netopia or from a site maintained by your organization's network administration.

Follow these steps to update the Netopia 4753's firmware:

1. Make sure you have the firmware file on disk and know the path to its location.
2. Select **Send Firmware to Netopia** and press Return. The following dialog box appears:



3. Select **CANCEL** to exit without downloading the file, or select **CONTINUE** to download the file.

If you choose CONTINUE, you will have ten seconds to use your terminal emulation software to initiate an XMODEM transfer of the firmware file. If you fail to initiate the transfer in that time, the dialog box will disappear and the terminal emulation software will inform you of the transfer's failure. You can then try again.

The system will reset at the end of a successful file transfer to put the new firmware into effect. While the system resets, the LEDs will blink on and off.

Caution!

Do not manually power down or reset the Netopia 4753 while it is automatically resetting or it could be damaged.

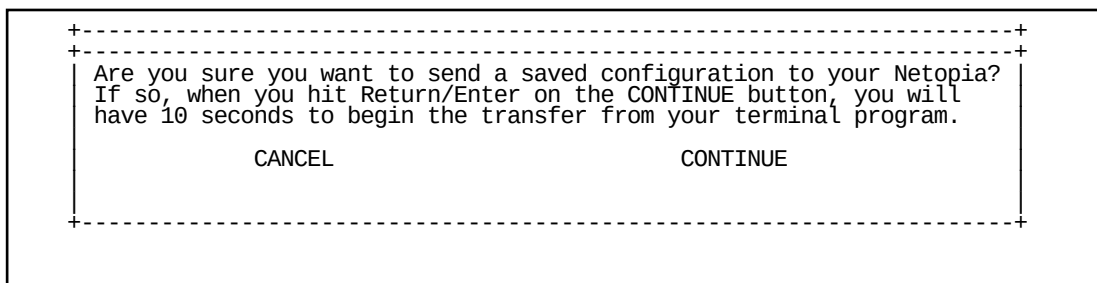
Downloading configuration files

The Netopia 4753 can be configured by downloading a configuration file. The downloaded file reconfigures all of the Router's parameters.

Configuration files are available from a site maintained by your organization's network administrator or from your local site (see ["Uploading configuration files,"](#) below).

Follow these steps to download a configuration file:

1. Make sure you have the configuration file on disk and know the path to its location.
2. Select **Send Config to Netopia** and press Return. The following dialog box appears:



3. Select **CANCEL** to exit without downloading the file, or select **CONTINUE** to download the file.

15-12 Administration Guide

If you choose CONTINUE, you will have ten seconds to use your terminal emulation software to initiate an XMODEM transfer of the configuration file. If you fail to initiate the transfer in that time, the dialog box will disappear and the terminal emulation software will inform you of the transfer's failure. You can then try again.

The system will reset at the end of a successful file transfer to put the new configuration into effect.

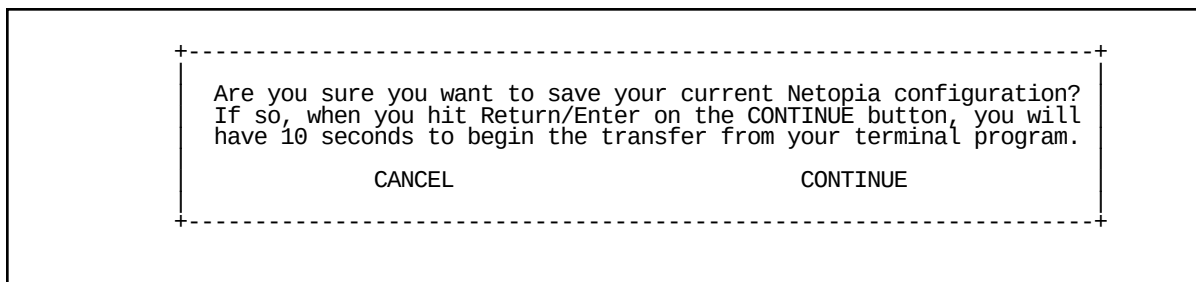
Uploading configuration files

A file containing a snapshot of the Netopia 4753's current configuration can be uploaded from the router to disk. The file can then be downloaded by a different Netopia 4753 to configure its parameters (see "[Downloading configuration files](#)," above). This is useful for configuring a number of routers with identical parameters or for creating configuration backup files.

Uploading a file can also be useful for troubleshooting purposes. The uploaded configuration file can be tested on a different Netopia 4753 by Netopia or your network administrator.

The procedure below applies whether you are using the console or the WAN interface. To upload a configuration file:

1. Decide on a name for the file and a path for saving it.
2. Select **Receive Config from Netopia** and press Return. The following dialog box appears:



Are you sure you want to save your current Netopia configuration?
If so, when you hit Return/Enter on the CONTINUE button, you will
have 10 seconds to begin the transfer from your terminal program.

CANCEL CONTINUE

3. Select **CANCEL** to exit without uploading the file, or select **CONTINUE** to upload the file.

If you choose CONTINUE, you will have ten seconds to use your terminal emulation software to initiate an XMODEM transfer of the configuration file. If you fail to initiate the transfer in that time, the dialog box will disappear and the terminal emulation software will inform you of the transfer's failure. You can then try again.

Restarting the System

You can restart the system by selecting the **Restart System** item in the Utilities & Diagnostics screen.

You must restart the system whenever you reconfigure the Netopia 4753 and want the new parameter values to take effect. Under certain circumstances, restarting the system may also clear up system or network malfunctions. Some configuration processes automatically restart the system to apply the changes you have made.

Part III: Appendixes

Appendix A

Troubleshooting

This appendix is intended to help you troubleshoot problems you may encounter while setting up and using the Netopia 4753. It also includes information on how to contact Netopia Technical Support.

Important information on these problems can be found in the event histories kept by the Netopia 4753. These event histories can be accessed in the Statistics & Logs screen.

This section covers the following topics:

- [“Configuration Problems” on page A-1](#)
- [“How to Reset the Netopia 4753 to Factory Defaults” on page A-3](#)
- [“Power Outages” on page A-3](#)
- [“Technical Support” on page A-4](#)

Configuration Problems

If you encounter problems during your initial configuration process, review the following suggestions before calling for technical support. There are five zones to consider when troubleshooting initial configuration:

1. The computer's connection to the Netopia 4753
2. The Netopia 4753's connection to the telecommunication line(s)
3. The telecommunication line's connection to your ISP
4. The ISP's connection to the Internet
5. The Netopia 4753's connection to the voice provider

If the connection from the computer to the Netopia 4753 was not successful, verify that the following conditions are in effect:

- The Netopia 4753 is turned on.
- An Ethernet cable connects your PC's Ethernet card or built-in Ethernet port to the Netopia 4753.
- Telnet is available on your PC or Macintosh. (On a PC, it must be specified in your system path. You can usually find the application as “c:\windows\telnet.exe”.)
- Your PC or Macintosh is properly configured for TCP/IP.
- Your PC or Macintosh has an IP address.
- Your PC or Macintosh has a subnet mask that matches or is compatible with the Netopia 4753's subnet mask.

Note: If you are attempting to modify the IP address or subnet mask from a previous, successful configuration attempt, you will need to clear the IP address or reset your Netopia 4753 to the factory default before reinitiating the configuration process. For further information on resetting your Netopia 4753 to factory default, see [“Factory Defaults” on page 15-6](#).

Console connection problems

Can't see the configuration screens (nothing appears)

- Make sure the cable connection from the Netopia 4753's console port to the computer being used as a console is securely connected.
- Make sure the terminal emulation software is accessing the correct port on the computer that's being used as a console.
- Try pressing Ctrl-L or Return or the up or down arrow key several times to refresh the terminal screen.
- Make sure that flow control on serial connections is turned off.

Junk characters appear on the screen

- Check that the terminal emulation software is configured correctly.
- Check the baud rate. The default values are 9600, N, 8, and 1.

Characters are missing from some of the configuration screens

- Try changing the Netopia 4753's default speed of 9600 bps and setting your terminal emulation software to match the new speed.

Network problems

Problems communicating with remote IP hosts

- Verify the accuracy of the default gateway's IP address (entered in the IP Setup or Easy Setup screen).
- Use the Netopia 4753's Ping utility, in the Utilities & Diagnostics screen, and try to Ping local and remote hosts. See [“Ping” on page 15-2](#) for instructions on how to use the Ping utility. If you can successfully Ping hosts using their IP addresses but not their domain names (198.34.7.1 but not garcia.netopia.com, for example), verify that the DNS server's IP address is correct and that it is reachable from the Netopia 4753 (use Ping).
- If you are using filters, check that your filter sets are not blocking the type of connections you are trying to make.

Local routing problems

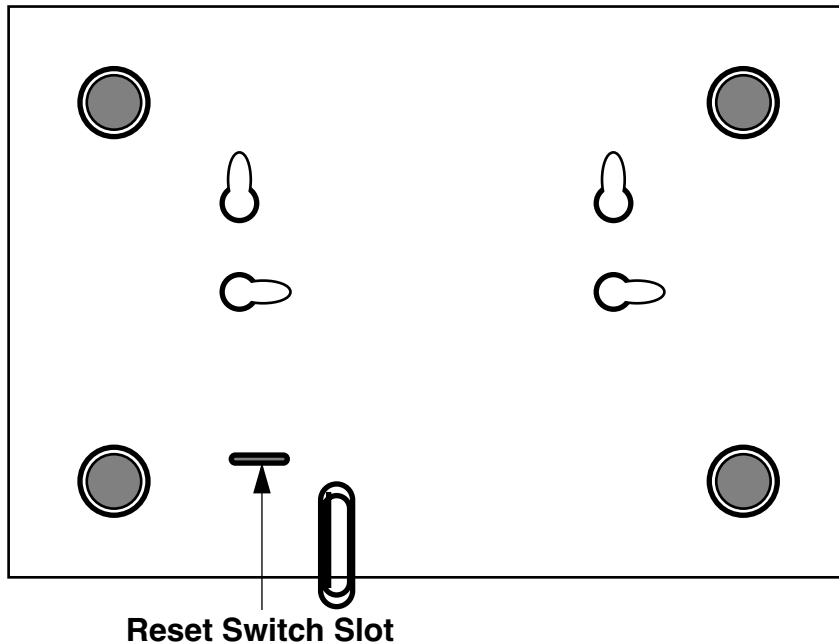
- Observe the Ethernet LEDs to see if data traffic flow appears to be normal.
- Check the WAN statistics and LAN statistics screens to see more specific information on data traffic flow and address serving. See [“Statistics & Logs” on page 14-4](#) for more information.

How to Reset the Netopia 4753 to Factory Defaults

Lose your password? This section shows how to reset the Netopia 4753 so that you can access the console screens once again. Keep in mind that all of your connection profiles and settings will need to be reconfigured.

If you don't have a password, the only way to get back into the Netopia 4753 is the following:

1. Turn the Netopia 4753 upside down.
2. Referring to the diagram below, find the paper clip-size Reset Switch slot.



3. Carefully insert the larger end of a standard size paper clip until you contact the internal Reset Switch. (No need to unwind the paper clip.)
4. Press this switch.
5. This will reset the unit to factory defaults and you will now be able to reprogram the Netopia 4753.

Power Outages

If you suspect that power was restored after a power outage and the Netopia 4753 is connected to a remote site, you may need to switch the Netopia 4753 off and then back on again. After temporary power outages, a connection that still seems to be up may actually be disconnected. Rebooting the Netopia 4753 should reestablish the connection.

Technical Support

Netopia, Inc. is committed to providing its customers with reliable products and documentation, backed by excellent technical support.

Before contacting Netopia

Look in this guide for a solution to your problem. You may find a solution in this troubleshooting appendix or in other sections. Check the index for a reference to the topic of concern. If you cannot find a solution, complete the environment profile below before contacting Netopia Technical Support.

Environment profile

- Locate the Netopia 4753's model number, product serial number, and firmware version. The serial number is on the bottom of the Netopia 4753, along with the model number. The firmware version appears in the Netopia 4753's Main Menu screen.

Model number:

Serial number:

Firmware version:

- What kind of local network(s) do you have, with how many devices?

Ethernet

TCP/IP

Other

- What kind of telephone(s) and/or fax machine(s) or other devices do you have, and how many each?

How to reach us

We can help you with your problem more effectively if you have completed the environment profile in the previous section. If you contact us by telephone, please be ready to supply Netopia Technical Support with the information you used to configure the Netopia 4753. Also, please be at the site of the problem and prepared to reproduce it and to try some troubleshooting steps.

When you are prepared, contact Netopia Technical Support by e-mail, telephone, fax, or post:

Internet: techsports@netopia.com (for technical support)

info@netopia.com (for general information)

Phone: 1 800-782-6449

Fax: 1 510-814-5023

Netopia, Inc.

Customer Service

2470 Mariner Square Loop

Alameda, California 94501

USA

Netopia Bulletin Board Service: 1 510-865-1321

Online product information

Product information can be found in the following:

Netopia World Wide Web server via <http://www.netopia.com>
Internet via anonymous FTP to <ftp.netopia.com/pub>

FAX-Back

This service provides technical notes that answer the most commonly asked questions and offers solutions for many common problems encountered with Netopia products.

FAX-Back: 1 510-814-5040

Appendix B

Understanding IP Addressing

This appendix is a brief general introduction to IP addressing. A basic understanding of IP will help you in configuring the Netopia 4753 and using some of its powerful features, such as static routes and packet filtering.

This section covers the following topics:

- “What is IP?” on page B-1
- “About IP Addressing” on page B-1
- “Distributing IP Addresses” on page B-5
- “Nested IP Subnets” on page B-11
- “Broadcasts” on page B-13

What is IP?

All networks use protocols to establish common standards for communication. One widely used network protocol is the Internet Protocol, also known as IP. Like many other protocols, IP uses packets, or formatted chunks of data, to communicate. In packets, a header is part of the envelope information that surrounds the actual data being transmitted. In e-mail, a header is usually the address and routing information found at the top of messages.

Note: This guide uses the term “IP” in a very general and inclusive way to identify all of the following:

- Networks that use the Internet Protocol, along with accompanying protocols such as TCP, UDP, and ICMP
- Packets that include an IP header within their structure
- Devices that send IP packets

About IP Addressing

Every networking protocol uses some form of addressing in order to ensure that packets are delivered correctly. In IP, individual network devices that are initial sources and final destinations of packets are usually called hosts instead of nodes, but the two terms are interchangeable. Each host on an IP network must have a unique IP address. An IP address, also called an Internet address, is a 32-bit number usually expressed as four decimal numbers separated by periods. Each decimal number in an IP address represents a 1-byte (8-bit) binary number. Thus, values for each of the four numbers range from 00000000 to 11111111 in binary notation, or from 0 to 255 in decimal notation. The expression 192.168.1.1 is a typical example of an IP address.

IP addresses indicate both the identity of the network and the identity of the individual host on the network. The number of bits used for the network number and the number of bits used for the host number can vary, as long as certain rules are followed. The local network manager assigns IP host numbers to individual machines.

B-2 Administration Guide

IP addresses are maintained and assigned by the InterNIC, a quasi-governmental organization now increasingly under the auspices of private industry.

Note: It's very common for an organization to obtain an IP address from a third party, usually an Internet service provider (ISP). ISPs usually issue an IP address when they are contracted to provide Internet access services.

The InterNIC (the NIC stands for Network Information Center) divides IP addresses into several classes. Classes A, B, and C are assigned to organizations that request addresses. In Class A networks, the first byte of an IP address is reserved for the network portion of the address. Class B networks reserve the first two bytes of an IP address for the network address. Class C networks reserve the first three bytes of an IP address for the network address. In all cases, a network manager can decide to use subnetting to assign even more bits to the network portion of the IP address, but never less than the class requires. The following section gives more information on subnetting.

Class A networks have a small number of possible network numbers, but a large number of possible host numbers. Conversely, Class C networks have a small number of possible host numbers, but a large number of possible network numbers. Thus, the InterNIC assigns Class A addresses to large organizations that have very large numbers of IP hosts, while smaller organizations, with fewer hosts, get Class B or Class C addresses. You can tell the various classes apart by the value of the first (or high-order) byte. Class A networks use values from 1 to 127, Class B networks use values from 128 to 191, and Class C networks use values from 192 to 223. The following table summarizes some of the differences between Class A, B, and C networks.

Class	First byte	Number of networks possible per class	Number of hosts possible per network	Format of address (without subnetting)	Example
A	1–127	127	16,777,214	net.host.host.host	97.3.14.250
B	128–191	16,384	65,534	net.net.host.host	140.100.10.11
C	192–223	2,097,152	254	net.net.net.host	197.204.13.7

Subnets and subnet masks

Often an entire organization is assigned only one IP network number. If the organization has several IP networks connected together with IP routers, the network manager can use subnetting to distinguish between these networks, even though they all use the same network number. Each physical network becomes a subnet with a unique subnet number.

Subnet numbers appear within IP addresses, along with network numbers and host numbers. Since an IP address is always 32 bits long, using subnet numbers means either the network number or the host numbers must use fewer bits in order to leave room for the subnet numbers. Since the InterNIC assigns the network number proper, it should not change, so the subnet numbers must be created out of bits that would otherwise be part of the host numbers.

Subnet masks

To create subnets, the network manager must define a subnet mask, a 32-bit number that indicates which bits in an IP address are used for network and subnetwork addresses and which are used for host addresses. One subnet mask should apply to all IP networks that are physically connected together and share a single assigned network number. Subnet masks are often written in decimal notation like IP addresses, but they are most easily understood in binary notation. When a subnet mask is written in binary notation, each numeral 1 indicates that the corresponding bit in the IP address is part of the network or subnet address. Each 0 indicates that the corresponding bit is part of the host address. The following table shows the proper subnet masks to use for each class of network when no subnets are required.

Class	Subnet mask for a network with no subnets
A	Binary: 11111111.00000000.00000000.00000000 Decimal: 255.0.0.0
B	Binary: 11111111.11111111.00000000.00000000 Decimal: 255.255.0.0
C	Binary: 11111111.11111111.11111111.00000000 Decimal: 255.255.255.0

To know whether subnets are being used or not, you must know what subnet mask is being used—you cannot determine this information simply from an IP address. Subnet mask information is configured as part of the process of setting up IP routers and gateways such as the Netopia 4753.

Note: If you receive a routed account from an ISP, there must be a mask associated with your network IP address. By using the IP address with the mask you can discover exactly how many IP host addresses you actually have.

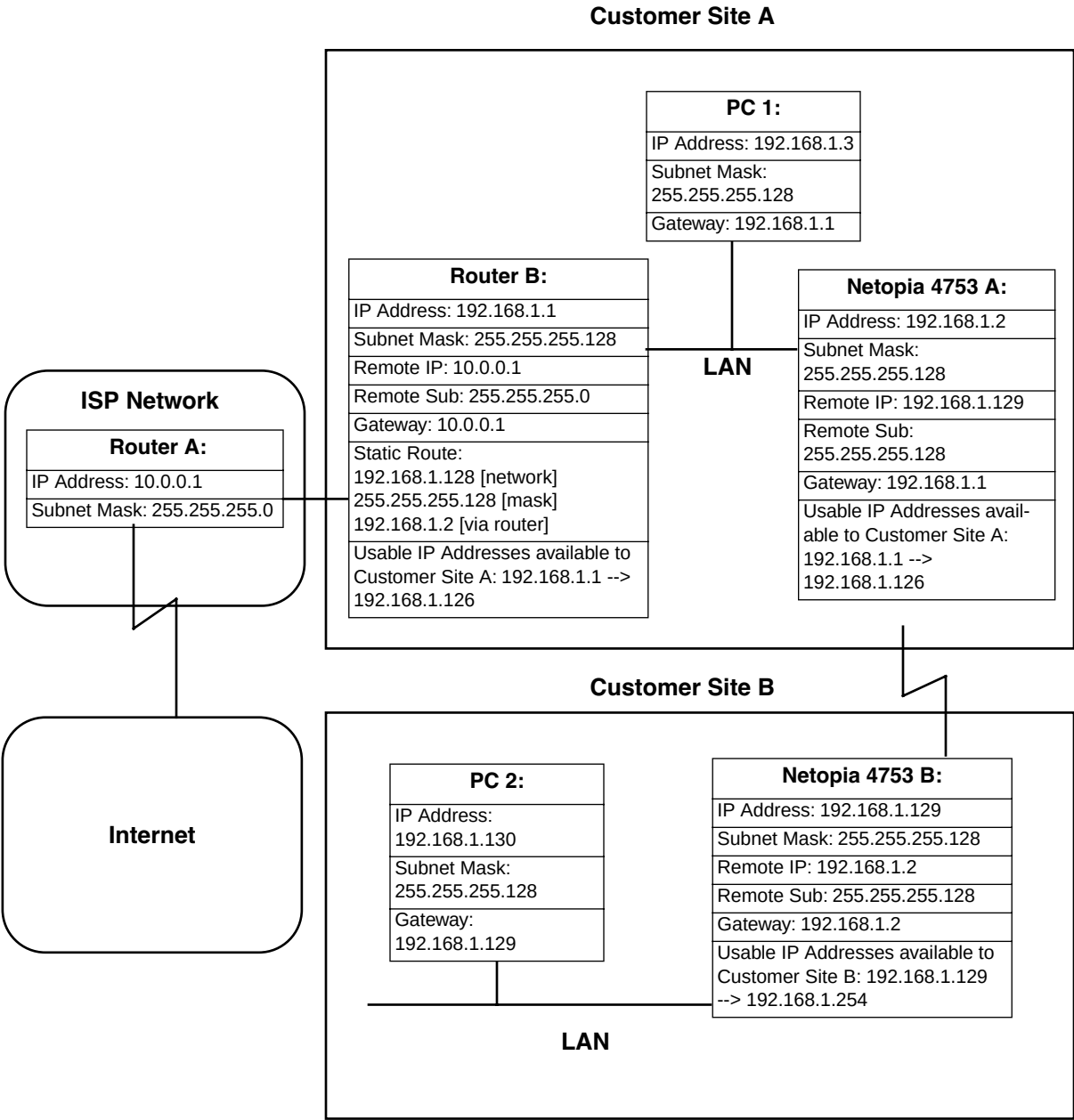
To configure subnets properly, you must also be able to convert between binary notation and decimal notation.

Example: Using subnets on a Class C IP internet

When setting up IP routing with a Class A address, or even with multiple Class C addresses, subnetting is fairly straightforward. Subnetting a single Class C address between two networks, however, is more complex. This section describes the general procedures for subnetting a single Class C network between two Netopia routers so that each can have Internet access.

Network configuration

Below is a diagram of a simple network configuration. The ISP is providing a Class C address to the customer site, and both networks A and B want to gain Internet access through this address. Netopia 4753 B connects to Netopia 4753 A and is provided Internet access through Routers A and B.



Background

The IP addresses and routing configurations for the devices shown in the diagram are outlined below. In addition, each individual field and its meaning are described.

The IP Address and Subnet Mask fields define the IP address and subnet mask of the device's Ethernet connection to the network while the Remote IP and Remote Sub fields describe the IP address and subnet mask of the remote router. This information is entered in the connection profile of the Netopia 4753.

The Gateway field describes the router or workstation's default gateway, or where they will send their packets if the appropriate route is not known. The Static Route field, which is only shown on Router B, tells Router B what path to take to get to the network defined by Netopia 4753 B. Finally, the Usable IP Address field shows the range of IP addresses available to the hosts of that network.

Note that the IP addresses given in this section are for example purposes only. Do not use these addresses when configuring your network.

With this configuration, both Customer Site A and B can gain Internet access through Routers A and B, with no reconfiguration of the ISP's equipment. The most important item in this configuration is the static route defined on Router B. This tells Router B what path to take to get to the network defined by Netopia 4753 B. Without this information, Customer Site B will be able to access Customer Site A, but not the Internet.

If it is not possible to define a static route on Router B, RIP could be enabled to serve the same purpose. To use RIP instead of a static route, enable Transmit RIP on Netopia 4753 A and Transmit and Receive RIP on Router B. This will allow the route from Customer Site B to propagate on Router B and Customer Site A.

Example: Working with a Class C subnet

Suppose that your organization has a site with only 10 hosts and no plans to add any new hosts. You don't need a full Class C address for this site. Many ISPs offer Internet access with only a portion of a full Internet address.

For example, you might obtain the Class C address 199.14.17.48, with the mask 255.255.255.240. From the previous example, you can see that this gives you 14 host addresses to distribute to the hosts at your site. In effect, your existing network of 10 hosts is a subnet of the ISP's network. Since the Class C address has already been reduced to subnets, you cannot further subnet your network without the risk of creating network routing problems (since you must use the mask issued by the ISP). This, however, is not a problematic limitation for your small network.

The advantages of this situation are the greater ease and lower cost of obtaining a subnet rather than a full Class C address from an ISP.

Distributing IP Addresses

To set up a connection to the Internet, you may have obtained a block of IP host addresses from an ISP. When configuring the Netopia 4753, you gave one of those addresses to its Ethernet port, leaving a number of addresses to distribute to computers on your network.

B-6 Administration Guide

There are two schemes for distributing the remaining IP addresses:

- Manually give each computer an address
- Let the Netopia 4753 automatically distribute the addresses

These two methods are not mutually exclusive; you can manually issue some of the addresses while the rest are distributed by the Netopia 4753. Using the router in this way allows it to function as an address server.

One reason to use the Netopia 4753 as an address server is that it takes less time than manually distributing the addresses. This is particularly true if you have many addresses to distribute. You need to enter information only once, rather than having to enter it on each host separately. This also reduces the potential for misconfiguring hosts.

Another reason to use the Netopia 4753 as an address server is that it will distribute addresses only to hosts that need to use them.

All Netopia 4753s come with an integrated Dynamic Host Control Protocol (DHCP) server. Some routers also come with a Macintosh Internet Protocol (MacIP) server. These servers provide a means of distributing IP addresses to either a Mac or PC workstation as needed.

When setting up the DHCP or MacIP servers in the Netopia 4753, it is necessary to understand how workstations lease, renew, and release their IP addresses. This information is helpful in determining dynamic address allocation for a network.

The term “lease” describes the action of a workstation requesting and using an IP address. The address is dynamic and can be returned to the address pool at a later time.

The term “renew” refers to what the workstations do to keep their leased IP address. At certain intervals, the workstation talks to the DHCP or MacIP server and renews the lease on that IP address. This renewal allows the workstation to keep and use the assigned IP address until the next renewal period.

The term “release” refers to a situation where the workstation is no longer using its assigned IP address or has been shut down. IP addresses can be manually released as well. The IP address goes back into the DHCP or MacIP address pool to be reassigned to another workstation as needed.

Technical note on subnet masking

Note: The IP address supplied by the Netopia 4753 will be a unique number. You may want to replace this number with a number that your ISP supplies if you are configuring the router for a static IP address. However, the Netopia 4753 and all devices on the same local network must have the same subnet mask. If you require a different class address, you can edit the IP Mask field to enter the correct address. Refer to the table below.

Number of Devices (other than Netopia 4753) on Local Network	Largest Possible Ethernet Subnet Mask
1	255.255.255.252
2-5	255.255.255.248 (6)
6-13	255.255.255.240 (14)
14-29	255.255.255.224 (30)
30-61	255.255.255.192

Number of Devices (other than Netopia 4753) on Local Network	Largest Possible Ethernet Subnet Mask
62-125	255.255.255.128
125-259	255.255.255.0

Configuration

This section describes the specific IP address lease, renew, and release mechanisms for both the Mac and PC, with either DHCP or MacIP address serving.

DHCP address serving

Windows 95 workstation:

- The Win95 workstation requests and renews its lease every half hour.
- The Win95 workstation does NOT relinquish its DHCP address lease when the machine is shut down.
- The lease can be manually expired using the WINIPCFG program, a command line program executable from the DOS prompt or from the START:RUN menu on a Windows-based computer.

Windows 3.1 workstation (MSTCP Version 3.11a):

- The Win3.1 workstation requests and renews its lease every half hour.
- The Win3.1 workstation does NOT relinquish its DHCP address lease when the user exits Windows and goes to DOS.
- The lease can be manually expired by typing IPCONFIG/RELEASE from a DOS window within Windows or from the DOS prompt.

Macintosh workstation (Open Transport Version 1.1 or later):

- The Mac workstation requests and renews its lease every half hour.
- The Mac workstation relinquishes its address upon shutdown in all but one case. If the TCP/IP control panel is set to initialize at startup, and no IP services are used or the TCP/IP control panel is not opened, the DHCP address will NOT be relinquished upon shutdown. However, if the TCP/IP control panel is opened or if an IP application is used, the Mac WILL relinquish the lease upon shutdown.
- If the TCP/IP control panel is set to acquire an address only when needed (therefore a TCP/IP application must have been launched to obtain a lease) the Mac WILL relinquish its lease upon shutdown every time.

Netopia 4753 DHCP server characteristics

- The Netopia 4753 ignores any lease-time associated with a DHCP request and automatically issues the DHCP address lease for one hour.
- The number of devices a Netopia 4753 can serve DHCP to is 512. This is imposed by global limits on the size of the address serving database, which is shared by all address serving functions active in the router.

B-8 Administration Guide

- The Netopia 4753 releases the DHCP address back to the available DHCP address pool exactly one hour after the last-heard lease request. Some other DHCP implementations may hold on to the lease for an additional time after the lease expired to act as a buffer for variances in clocks between the client and server.

MacIP serving

Macintosh workstation (MacTCP or Open Transport):

Once the Mac workstation requests and receives a valid address, the Netopia 4753 actively checks for the workstation's existence once every minute.

- For a dynamic address, the Netopia 4753 releases the address back to the address pool after it has lost contact with the Mac workstation for over 2 minutes.
- For a static address, the Netopia 4753 releases the address back to the address pool after it has lost contact with the Mac workstation for over 20 minutes.

Netopia 4753 MacIP server characteristics

The Mac workstation uses ATP to both request and receive an address from the Netopia 4753's MacIP server. Once acquired, NBP confirm packets will be sent out every minute from the Netopia 4753 to the Mac workstation.

Manually distributing IP addresses

If you choose to manually distribute IP addresses, you must enter each computer's address into its TCP/IP stack software. Once you manually issue an address to a computer, it possesses that address until you manually remove it. That's why manually distributed addresses are called static addresses.

Static addresses are useful in cases when you want to make sure that a host on your network cannot have its address taken away by the address server. Appropriate candidates for a static address include a network administrator's computer, a computer dedicated to communicating with the Internet, and routers.

Using address serving

The Netopia 4753 provides three ways to serve IP addresses to computers on a network. The first, Dynamic Host Configuration Protocol (DHCP), is supported by PCs with Microsoft Windows and a TCP/IP stack. Macintosh computers using Open Transport and computers using the UNIX operating system may also be able to use DHCP. The second way, MacIP, is for Macintosh computers. The third way, called Serve Dynamic WAN Clients (IPCP), is used to fulfill WAN client requirements.

The Netopia 4753 can use both DHCP and MacIP. Whether you use one or both depends on your particular networking environment. If that environment includes both PCs and Macintosh computers that do not use Open Transport, you need to use both DHCP and MacIP to distribute IP addresses to all of your computers.

Serve dynamic WAN clients

The third method, used to fulfill WAN client requirements, is called Serve Dynamic WAN Clients. The correct term or protocol is a subset of the PPP suite call IPCP. Originally, this would apply only to switched WAN interface routers, and not to leased line routers. However, a new feature can give you Asynchronous PPP dial-in support on the Auxiliary port on any router including leased line Netopia routers.

In any situation where a device is dialing into a Netopia router, the router may need to be configured to serve IP via the WAN interface. This is only a requirement if the calling device has not been configured locally to know what its address(es) are. So when a client, dialing into a Netopia router's WAN interface, is expecting addresses to be served by the answering router, you must set the answering Netopia router to serve IP via its WAN interface.

You can do this in either of two ways:

- use the Serve Dynamic WAN Clients option in the Address Serving Setup screen.

Enabling Serve Dynamic WAN Clients only allows you to specify a pool of addresses from which the dial-in client may get an IP address. It does not allow static addressing.

If you want to serve addresses dynamically, use Serve Dynamic WAN Clients.

- define the address that you want to serve in the Connection Profile's IP Setup screen.

This method requires a static value to be used. Thus any user dialing in can obtain the same IP address for every connection to the profile.

If you want to serve addresses statically, define the address in the Connection Profile.

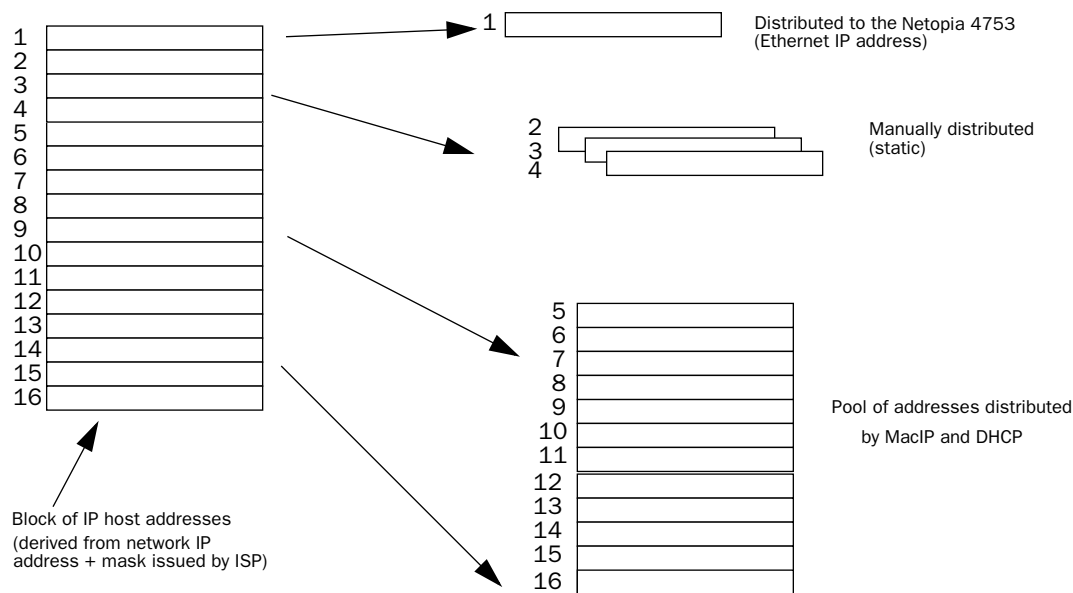
Notes:

- The addresses that are to be served cannot be used elsewhere. For example you wouldn't want to define a static address in a Connection Profile to be served via the WAN that is already defined in the DHCP pool of addresses.
- In order to work correctly, you must define a host or node address in the IP Profile Parameters of the Connection Profile.

This is accomplished by specifying the IP address that is to be statically served via the WAN, and then by entering a mask value of 255.255.255.255.

Tips and rules for distributing IP addresses

- Before you allocate IP addresses using DHCP and MacIP, consider whether you need to set aside any static addresses.
- Note any planned and currently used static addresses before you use DHCP and MacIP.
- Avoid fragmenting your block of IP addresses. For example, try to use a continuous range for the static addresses you choose.



The figure above shows an example of a block of IP addresses being distributed correctly.

The example follows these rules:

- An IP address must not be used as a static address if it is also in a range of addresses being distributed by DHCP or MacIP.
- A single IP address range is used by all the address-served clients. These include DHCP, BootP, MacIP, and WAN clients, even though BootP and static MacIP clients might not be considered served.
- The address range specified for address-served clients cannot wrap around from the end of the total available range back to the beginning. See below for a further explanation and an example.
- The network address issued by an ISP cannot be used as a host address.

A DHCP example

Suppose, for example, that your ISP gave your network the IP address 199.1.1.32 and a 4-bit subnet mask. Address 199.1.1.32 is reserved as the network address. Address 199.1.1.47 is reserved as the broadcast address. This leaves 14 addresses to allocate, from 199.1.1.33 through 199.1.1.46. If you want to allocate a sub-block of 10 addresses using DHCP, enter “10” in the DHCP Setup screen’s **Number of Addresses to Allocate** item. Then, in the same screen’s **First Address** item, enter the first address in the sub-block to allocate so that all 10 addresses are within your original block. You could enter 199.1.1.33, or 199.1.1.37, or any address between them. Note that if you entered 199.1.1.42 as the first address, network routing errors would probably result because you would be using a range with addresses that do not belong to your network (199.1.1.49, 199.1.1.50, and 199.1.1.51). The DHCP server would not initialize if set incorrectly.

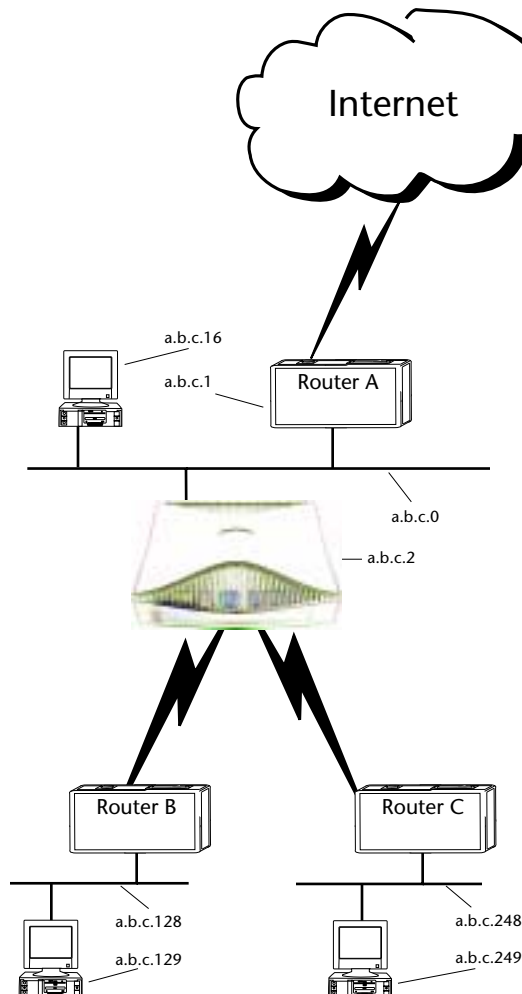
Nested IP Subnets

Under certain circumstances, you may want to create remote subnets from the limited number of IP addresses issued by your ISP or other authority. You can do this using connection profiles. These subnets can be nested within the range of IP addresses available to your network.

For example, suppose that you obtain the Class C network address a.b.c.0 to be distributed among three networks. This network address can be used on your main network, while portions of it can be subnetted to the two remaining networks.

Note: The IP address a.b.c.0 has letters in place of the first three numbers to generalize it for this example.

The figure shows a possible network configuration following this scheme. The main network is set up with the Class C address a.b.c.0, and contains Router A (which could be a Netopia 4753), a Netopia 4753, and a number of other hosts. Router A maintains a link to the Internet and can be used as the default gateway.



B-12 Administration Guide

Routers B and C (which could also be Netopia 4753s) serve the two remote networks that are subnets of a.b.c.0. The subnetting is accomplished by configuring the Netopia 4753 with connection profiles for Routers B and C (see the following table).

Connection profile	Remote IP address	Remote IP mask	Bits available for host address
For Router B	a.b.c.128	255.255.255.192	7
For Router C	a.b.c.248	255.255.255.248	3

The Netopia 4753’s connection profiles for Routers B and C create entries in its IP routing table. One entry points to the subnet a.b.c.128, while a second entry points to the subnet a.b.c.248. The IP routing table might look similar to the following:

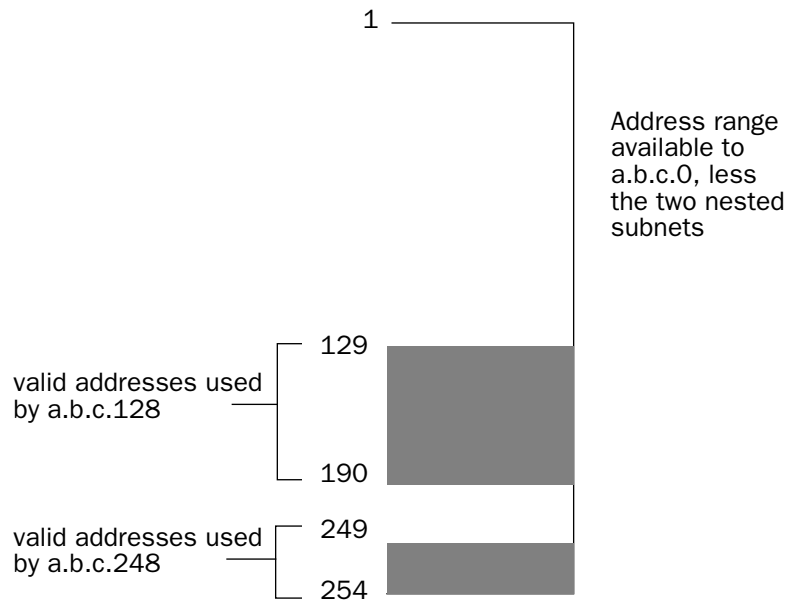
IP Routing Table					
Network	Address-Subnet	Mask-----	via Router-----	Port-----	Type-----
-----SCROLL UP-----					
0.0.0.0	0.0.0.0		a.b.c.1	--	Other
127.0.0.1	255.255.255.255		127.0.0.1	Loopback	Local
a.b.c.128	255.255.255.192		a.b.c.128	WAN	Local
a.b.c.248	255.255.255.248		a.b.c.248	WAN	Local
-----SCROLL DOWN-----					
UPDATE					

Let’s see how a packet from the Internet gets routed to the host with IP address a.b.c.249, which is served by Router C. The packet first arrives at Router A, which delivers it to its local network (a.b.c.0). The packet is then received by the Netopia 4753, which examines its destination IP address.

The Netopia 4753 compares the packet’s destination IP address with the routes in its IP routing table. It begins with the route at the bottom of the list and works up until there’s a match or the route to the default gateway is reached.

When a.b.c.249 is masked by the first route’s subnet mask, it yields a.b.c.248, which matches the network address in the route. The Netopia 4753 uses the connection profile associated with the route to connect to Router C, and then forwards the packet. Router C delivers the packet to the host on its local network.

The following diagram illustrates the IP address space taken up by the two remote IP subnets. You can see from the diagram why the term nested is appropriate for describing these subnets.



Broadcasts

As mentioned earlier, binary IP host or subnet addresses composed entirely of ones or zeros are reserved for broadcasting. A broadcast packet is a packet that is to be delivered to every host on the network if both the host address and the subnet address are all ones or all zeros, or to every host on the subnetwork if the host address is all ones or all zeros but the subnet address is a combination of zeros and ones. Instead of making many copies of the packet, individually addressed to different hosts, all the host machines know to pay attention to broadcast packets, as well as to packets addressed to their specific individual host addresses. Depending on the age and type of IP equipment you use, broadcasts will be addressed using either all zeros or all ones, but not both. If your network requires zeros broadcasting, you must configure this through SNMP.

Packet header types

As previously mentioned, IP works with other protocols to allow communication over IP networks. When IP is used on an Ethernet network, IP works with the Ethernet or 802.3 framing standards, among other protocols. These two protocols specify two different ways to organize the very first signals in the sequence of electrical signals that make up an IP packet travelling over Ethernet. By default, the Netopia 4753 uses Ethernet packet headers for IP traffic. If your network requires 802.3 IP framing, you must configure this through SNMP.

Appendix C

Binary Conversion Table

This table is provided to help you choose subnet numbers and host numbers for IP and MacIP networks that use subnetting for IP addresses.

Decimal	Binary	Decimal	Binary	Decimal	Binary	Decimal	Binary
0	0	32	100000	64	1000000	96	1100000
1	1	33	1000001	65	1000001	97	1100001
2	10	34	100010	66	1000010	98	1100010
3	11	35	100011	67	1000011	99	1100011
4	100	36	100100	68	1000100	100	1100100
5	101	37	100101	69	1000101	101	1100101
6	110	38	100110	70	1000110	102	1100110
7	111	39	100111	71	1000111	103	1100111
8	1000	40	101000	72	1001000	104	1101000
9	1001	41	101001	73	1001001	105	1101001
10	1010	42	101010	74	1001010	106	1101010
11	1011	43	101011	75	1001011	107	1101011
12	1100	44	101100	76	1001100	108	1101100
13	1101	45	101101	77	1001101	109	1101101
14	1110	46	101110	78	1001110	110	1101110
15	1111	47	101111	79	1001111	111	1101111
16	10000	48	110000	80	1010000	112	1110000
17	10001	49	110001	81	1010001	113	1110001
18	10010	50	110010	82	1010010	114	1110010
19	10011	51	110011	83	1010011	115	1110011
20	10100	52	110100	84	1010100	116	1110100
21	10101	53	110101	85	1010101	117	1110101
22	10110	54	110110	86	1010110	118	1110110
23	10111	55	110111	87	1010111	119	1110111
24	11000	56	111000	88	1011000	120	1111000
25	11001	57	111001	89	1011001	121	1111001
26	11010	58	111010	90	1011010	122	1111010
27	11011	59	111011	91	1011011	123	1111011
28	11100	60	111100	92	1011100	124	1111100
29	11101	61	111101	93	1011101	125	1111101
30	11110	62	111110	94	1011110	126	1111110
31	11111	63	111111	95	1011111	127	1111111

Decimal	Binary	Decimal	Binary	Decimal	Binary	Decimal	Binary
128	10000000	160	10100000	192	11000000	224	11100000
129	10000001	161	10100001	193	11000001	225	11100001
130	10000010	162	10100010	194	11000010	226	11100010
131	10000011	163	10100011	195	11000011	227	11100011
132	10000100	164	10100100	196	11000100	228	11100100
133	10000101	165	10100101	197	11000101	229	11100101
134	10000110	166	10100110	198	11000110	230	11100110
135	10000111	167	10100111	199	11000111	231	11100111
136	10001000	168	10101000	200	11001000	232	11101000
137	10001001	169	10101001	201	11001001	233	11101001
138	10001010	170	10101010	202	11001010	234	11101010
139	10001011	171	10101011	203	11001011	235	11101011
140	10001100	172	10101100	204	11001100	236	11101100
141	10001101	173	10101101	205	11001101	237	11101101
142	10001110	174	10101110	206	11001110	238	11101110
143	10001111	175	10101111	207	11001111	239	11101111
144	10010000	176	10110000	208	11010000	240	11110000
145	10010001	177	10110001	209	11010001	241	11110001
146	10010010	178	10110010	210	11010010	242	11110010
147	10010011	179	10110011	211	11010011	243	11110011
148	10010100	180	10110100	212	11010100	244	11110100
149	10010101	181	10110101	213	11010101	245	11110101
150	10010110	182	10110110	214	11010110	246	11110110
151	10010111	183	10110111	215	11010111	247	11110111
152	10011000	184	10111000	216	11011000	248	11111000
153	10011001	185	10111001	217	11011001	249	11111001
154	10011010	186	10111010	218	11011010	250	11111010
155	10011011	187	10111011	219	11011011	251	11111011
156	10011100	188	10111100	220	11011100	252	11111100
157	10011101	189	10111101	221	11011101	253	11111101
158	10011110	190	10111110	222	11011110	254	11111110
159	10011111	191	10111111	223	11011111	255	11111111

Appendix D

Further Reading

Alexander, S. and R. Droms, *DHCP Options and BOOTP Vendor Extensions*, RFC 2131, Silicon Graphics, Inc., Bucknell University, PA, 1997.

Black, U., *Data Networks: Concepts, Theory and Practice*, Prentice Hall, Englewood Cliffs, NJ, 1989.

Black, U., *Physical Level Interfaces and Protocols*, IEEE Computer Society Press, Los Alamitos, CA, 1988.

Black, U., *Emerging Communications Technologies*, PTR Prentice Hall, Englewood Cliffs, NJ, 1994. Describes how emerging communications technologies, including ISDN and Frame Relay, operate and where they fit in a computer/communications network.

Bradley, T., C. Brown and A. Malis, *Multiprotocol Interconnect over Frame Relay*, Network Working Group, Internet Engineering Task Force, RFC 1490, 1993.

Case, J.D., J.R. Davins, M.S. Fedor, and M.L. Schoffstall, *Introduction to the Simple Gateway Monitoring Protocol*, IEEE Network, March 1988.

Case, J.D., J.R. Davins, M.S. Fedor, and M.L. Schoffstall, *Network Management and the Design of SNMP, ConneXions: The Interoperability Report*, Vol. 3, March 1989.

Chapman, D. Brent, *Network (In)Security Through IP Packet Filtering*, Great Circle Associates, Mountain View, CA.

Chapman, D. Brent, and Elizabeth D. Zwicky, *Building Internet Firewalls*, O'Reilly & Associates, Sebastopol, CA, 1995. Dense and technical, but Chapter 6 provides a basic introduction to packet filtering.

Clark, W., *SNA Internetworking, ConneXions: The Interoperability Report*, Vol. 6, No. 3: March 1992.

Comer, D.E., *Internetworking with TCP/IP: Principles, Protocols, and Architecture* Vol. I, 2nd ed., Prentice Hall, Englewood Cliffs, NJ, 1991.

Copper Mountain Networks, Internal Control Protocol (ICP) Interface Control Document (ICD), January 5, 1998.

Davidson, J., *An Introduction to TCP/IP*, Springer-Verlag, New York, NY, 1992.

Droms, R., *Dynamic Host Configuration Protocol*, RFC 2131, Bucknell University, PA, 1997.

Ferrari, D., *Computer Systems Performance Evaluation*, Prentice Hall, Englewood Cliffs, NJ, 1978.

Garcia-Luna-Aceves, J.J., *Loop-Free Routing Using Diffusing Computations*, IEEE/ACM Transactions on Networking, Vol. 1, No. 1, 1993.

Garfinkel, Simson., *PGP: Pretty Good Privacy*, O'Reilly & Associates, Sebastopol, CA, 1991. A guide to the free data encryption program PGP and the issues surrounding encryption.

Green, J.K., *Telecommunications*, 2nd ed., Business One Irwin, Homewood, IL, 1992.

Heinanen, J., *Multiprotocol Encapsulation over ATM Adaptation Layer 5*, RFC 1483, July 1993.

Jones, N.E.H., and D. Kosiur., *MacWorld Networking Handbook*, IDG Books Worldwide, Inc., San Mateo, CA, 1992.

Kousky, K., *Bridging the Network Gap, LAN Technology*, Vol. 6, No. 1, January 1990.

D-2 Administration Guide

LaQuey, Tracy, *The Internet Companion: A Beginner's Guide to Global Networking*, Addison-Wesley Publishing Company, Reading, MA, 1994.

Leinwand, A., and K. Fang, *Network Management: A Practical Perspective*, Addison-Wesley Publishing Company, Reading, MA, 1993.

Levine, John R., and Carol Baroudi, *The Internet for Dummies*, IDG Books Worldwide, Foster City, CA, 1993. Covers all of the most popular Internet services, including e-mail, newsgroups, and the World Wide Web. Also has information on setting up individual workstations with TCP/IP stacks.

Lippis, N., *The Internetwork Decade, Data Communications*, Vol. 20, No. 14: October 1991.

McNamara, J.E., *Local Area Networks*. Digital Press, Educational Services, Digital Equipment Corporation, Bedford, MA 01730.

Malamud, C., *Analyzing Sun Networks*, Van Nostrand Reinhold, New York, NY, 1991.

Martin, J., *SNA: IBM's Networking Solution*, Prentice Hall, Englewood Cliffs, NJ, 1987.

Martin, J., with K.K. Chapman and the ARBEN Group, Inc., *Local Area Networks: Architectures and Implementations*, Prentice Hall, Englewood Cliffs, NJ, 1989.

Miller, A. Mark, *Analyzing Broadband Networks (Frame Relay, SMDS, & ATM)*, M&T Books, San Mateo, CA, 1994. An intermediate/advanced reference on Frame Relay technologies.

Miller, M.A., *Internetworking: A Guide to Network Communications LAN to LAN; LAN to WAN*, 2nd. ed., M&T Books, San Mateo, CA, 1992.

Miller, M.A., *LAN Protocol Handbook*, M&T Books, San Mateo, CA, 1990.

Miller, M.A., *LAN Troubleshooting Handbook*, M&T Books, San Mateo, CA, 1989.

Perlman, R., *Interconnections: Bridges and Routers*, Addison-Wesley Publishing Company, Reading, MA, 1992.

Rose, M.T., *The Open Book: A Practical Perspective on OSI*, Prentice Hall, Englewood Cliffs, NJ, 1990.

Rose, M.T., *The Simple Book: An Introduction to Management of TCP/IP-based Internets*, Prentice Hall, Englewood Cliffs, NJ, 1991.

Schwartz, M., *Telecommunications Networks: Protocols, Modeling, and Analysis*, Addison-Wesley Publishing Company, Reading, MA, 1987.

Sherman, K., *Data Communications: A User's Guide*, Prentice Hall, Englewood Cliffs, NJ, 1990.

Sidhu, G.S., R.F. Andrews, and A.B. Oppenheimer, *Inside AppleTalk*, 2nd ed., Addison-Wesley Publishing Company, Reading, MA, 1990.

Siyam, Karanjit, *Internet Firewall and Network Security*, New Riders Publishing, Indianapolis, IN, 1995. Similar to the Chapman and Zwicky book.

Smith, Philip, *Frame Relay Principles and Applications*, Addison-Wesley Publishing Company, Reading, MA, 1996. Covers information on Frame Relay, including the pros and cons of the technology, description of the theory and application, and an explanation of the standardization process.

Spragins, J.D., et al., *Telecommunications Protocols and Design*, Addison-Wesley Publishing Company, Reading, MA, 1991.

Stallings, W., *Data and Computer Communications*, Macmillan Publishing Company, New York, NY, 1991.

Stallings, W., *Handbook of Computer-Communications Standards*, Vols. 1–3, Howard W. Sams, Carmel, IN, 1990.

- Stallings, W. *Local Networks*, 3rd ed., Macmillan Publishing Company, New York, NY, 1990.
- Stevens, W.R., *TCP/IP Illustrated*, Vol 1, Addison-Wesley Publishing Company, Reading, MA, 1994.
- Sunshine, C.A. (ed.), *Computer Network Architectures and Protocols*, 2nd ed., Plenum Press, New York, NY, 1989.
- Tannenbaum, A.S., *Computer Networks*, 2nd ed., Prentice Hall, Englewood Cliffs, NJ, 1988.
- Terplan, K., *Communication Networks Management*, Prentice Hall, Englewood Cliffs, NJ, 1992.
- Tsuchiya, P., *Components of OSI: IS-IS Intra-Domain Routing*, *ConneXions: The Interoperability Report*, Vol. 3, No. 8: August 1989.
- Tsuchiya, P., *Components of OSI: Routing (An Overview)*, *ConneXions: The Interoperability Report*, Vol. 3, No. 8: August 1989.
- Zimmerman, H., *OSI Reference Model—The ISO Model of Architecture for Open Systems Interconnection*, *IEEE Transactions on Communications COM-28*, No. 4: April 1980.

Appendix E

Technical Specifications and Safety Information

Description

Dimensions: 130.48 cm (w) x 24.13 cm (d) x 4.445 cm (h)
12" (w) x 9.5" (d) x 1.75" (h)

Communications interfaces: The Netopia 4753 G.SHDSL Integrated Access Device has an RJ-45 jack for G.SHDSL line connections; a 10/100Base-T Ethernet port for your LAN connection; 8 telephone extension jacks; and a DB-9 Console port.

Power requirements

- 12 VDC input
- 1.5 amps

Environment

Operating temperature: 0° to +40° C

Storage temperature: 0° to +70° C

Relative storage humidity: 20 to 80% noncondensing

Software and protocols

Software media: Software preloaded on internal flash memory; field upgrades done via download to internal flash memory via XMODEM or TFTP

Routing: TCP/IP Internet Protocol Suite, RIP

WAN support: G.SHDSL

Security: IP firewalls, UI password security, PAP, CHAP.

SNMP network management: SNMPv1, MIB-II (RFC 1213), Interface MIB (RFC 1229), Ethernet MIB (RFC 1643), Netopia 4753 MIB

Management/configuration methods: Serial console, remote modem console, Telnet, SNMP

Diagnostics: Ping, event logging, routing table displays, trace route, statistics counters

Agency Approvals

North America

Safety Approvals:

- United States – UL Standard for Information Technology Equipment, UL 60950, Third Edition, Dated December 1, 2000
- Canada – CSA: CAN/CSA-C22.2 No. 950-95

EMI:

- FCC Part 15 Class B

International

Safety Approvals:

- Low Voltage (European directive) 73/23/EEC
- EN60950 1992 (Europe)
- AS/NRZ 3260 (Australia)
- TS001(Australia)

EMI Compatibility:

- European Directive 89/336/EEC
- EN 300 368.2-1997

Telco:

- European Directive 1999/5/EC

Regulatory notices

Warning

This is a Class B product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures. Adequate measures include increasing the physical distance between this product and other electrical devices.

United States. This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Service requirements. In the event of equipment malfunction, all repairs should be performed by our Company or an authorized agent. Under FCC rules, no customer is authorized to repair this equipment. This restriction applies regardless of whether the equipment is in or out of warranty. It is the responsibility of users requiring service to report the need for service to our Company or to one of our authorized agents. Service can be obtained at Netopia, Inc., 2470 Mariner Square Loop, Alameda, California, 94501.

Important

This product was tested for FCC compliance under conditions that included the use of shielded cables and connectors between system components. Changes or modifications to this product not authorized by the manufacturer could void your authority to operate the equipment.

Canada. This digital apparatus does not exceed the Class B limits for radio noise emission from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Règlement sur le brouillage radioélectrique édicté par le ministère des Communications du Canada.

Declaration for Canadian users

The Canadian Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operation, and safety requirements. The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single line individual service may be extended by means of a certified connector assembly (telephone extension cord). The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to the certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment or equipment malfunctions may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution. Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

The load number (LN) assigned to each terminal device denotes the percentage of the total load to be connected to a telephone loop that is used by the device to prevent overloading. The termination on a loop may consist of any combination of devices subject only to the requirement that the total of the load numbers of all the devices does not exceed 100.

Important Safety instructions

CAUTIONS

CAUTION: Depending on the power supply provided with the product, either the direct plug-in power supply blades, power supply cord plug or the appliance coupler serves as the mains power disconnect. It is important that the direct plug-in power supply, socket-outlet or appliance coupler be located so it is readily accessible.

CAUTION (North America Only): For use only with a CSA Certified or UL Listed Limited Power Source or Class 2 power supply, rated 12Vdc, 1.5A.

CAUTION (Europe Only): For use only with a GS approved Limited Power Source, rated 12Vdc, 1.5A.

TELECOMMUNICATION INSTALLATION CAUTIONS

When using your telephone equipment, basic safety precautions should always be followed to reduce the risk of fire, electric shock and injury to persons, including the following:

1. Do not use this product near water, for example, near a bathtub, wash bowl, kitchen sink or laundry tub, in a wet basement or near a swimming pool.
2. Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electrical shock from lightning.
3. Do not use the telephone to report a gas leak in the vicinity of the leak.

SAVE THESE INSTRUCTIONS

Netopia 4753 Specifications

Physical interface

WAN interface

- G.SHDSL port with support for symmetric connections from 64 Kbps to 2.368 Mbps (uses RJ68 connector)
- Interoperable with G.SHDSL equipment from Ericsson and others.

LAN interface

10/100BaseT Ethernet port

Voice interfaces

- 8 Analog loopstart telephone interfaces (RJ11) for connection to phone handsets or fax.
- Supports optional FSK Caller ID and message waiting
- Supports G.711 64 Kbps PCM and G.726 32 Kbps ADPCM
- Interoperable with VoDSL equipment from Jetstream, CopperCom, Zhone, TdSoft, and Tollbridge

Management interface

- Console port for direct access to console management screens or CLI
- In band management via Telnet to console management screens, CLI, also SNMP

Data features

Routing

- Network Protocols: IP routing
- Dynamic Host Configuration Protocol (DHCP) Server (RFC 2131), Client (RFC 2131) and Relay Agent (RFC 1542)
- NAT/NAPT: (Network Address and Network Address Port Translation (RFC 1631) Port Translation allows mail, Web, PPTP, IPsec and other servers on the LAN to be accessible from the Internet
- MultiNAT: Sophisticated NAT extension that provides security of a NAT “wall” to hide LAN IP addresses on LAN while providing flexible use of all addresses offered by an ISP
- RADIUS Client support for authenticating system configuration access
- Built-in Firewall: Pre-configured firewall to disallow all inbound traffic originated from the internet; Includes IP filtering; Filter packets on a per-connection profile basis for source/destination address, service, and protocol. Up to 255 rules in up to 8 filter sets.
- Secure VPN: ATMP client and server, PPTP client (PAC) and server (PNS), PPTP NAT pass through, IPsec with DES

E-6 Administration Guide

Protocols

- ATM Protocols: ATM Multiprotocol Encapsulation over ATM Adaption Layer 5 (RFC 1483): Logical Link Control (LLC) encapsulation routed modes
- Support for up to 8 ATM PVCs and 16 Frame Relay PVCs
- PPP Over ATM, PPP over Ethernet: PAP, CHAP or no authentication (RFC 2364). Compression Control Protocol (RFC 1974)
- Frame Relay Supports: ANSI T1.617 and ANSI T1.618 Annex D LMI, Annex A and Cisco LMI, (RFC 1490) multiprotocol Interconnect over Frame Relay. FRF.12 Fragmentation.
- Compression: IP Control Protocol (RFC 1332), PPP Stac LZS Compression Protocol (RFC 1974), Ascend LZS Compression Protocol, Van Jacobson Header Compression
- Virtual Circuit: Terminates ATM Permanent Virtual Circuit (PVC) with ATM Adaptation Layer 5 (AAL5); Allows manual configuration of Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI). Supports Multiple PVCs, and multiple VCI/VPI support.
- Routing: Transmit and Receive RIPv1 and RIPv2 (RFC 2453) and RIPv1 compatibility mode, up to 32 static routes with default route and the option to not advertise routes, configurable with up to 8 subnets on LAN with DHCP pool associated with each subnet
- IP Addressing: Dynamic Host Configuration Protocol (DHCP) and BootP servers. Supports up to 8 different pools of IP addresses (one per subnet) with a maximum of 512 addresses.
- WAN IP Interface: Numbered or Unnumbered Interface

Quality of service

- TOS Bit Type of Service or application based queuing.
- Frame Relay: FRF.12 support
- ATM: UBR, CBR, VBR-rt support

Management

- (with G.HSDSLAMs): Automatically hunts through available speed modes until successfully trains at the speed set by remote DSL concentrator
- Management Security: Password-protected with up to 4 user names and passwords
- LEDs: Diagnostic lights for at-a-glance management of Ethernet, WAN, phone and power connections
- Firmware: Upgrade firmware in flash memory via TFTP or X-Modem transfer using modem or direct cable connection; configuration retained with upgrades; battery backup to protect configuration across power failures
- Trivial File Transfer Protocol (TFTP) Client: Allows remote upload and download firmware and configuration files directly to the router
- Integrated Management Utilities: ICMP Ping: Tests IP connectivity from router to local or remote site. Trace Route: Determines routing path to particular host name or IP address. Telnet Client: Provides remote management access to Telnet hosts on the LAN and WAN. Syslog Client: Maintains ongoing activity log on

a syslog server

- SNMPv1: (RFC 1157) and MIB II (RFC 1213), Ethernet MIB and enterprise MIB for remote management using console applications

Hardware specifications

- Memory: 16 MB DRAM memory
- Environmental Requirement: Operating: 0° to +40° C. Storage: 0° to +70° C (20 to 80% non-condensing)
- Power Requirements: AC 100-240 V; 50/60 Hz; 1.66A
- Dimensions: 11.8" (299.7 mm) Wide X 1.7" (43.2 mm) High X 9.2" (233.7 mm) Long
- Weight: 2.25 lb. (1.03 kg) (unit carton)
- UL Listed, CSA Approved, FCC part 15, Class B

Voice features

POTS support

- Touch-tone support
- Direct Outward Dialing (DOD) provides dial tone for outside calling to any connected extension
- CallerID support with connected CallerID equipment, delivers name and telephone number during call waiting
- Selective Compression Each port configurable for either 64 Kbps PCM or 32 Kbps ADPCM

Voice quality

- G.168 echo cancellation, 16 millisecond fixed tail length
- Crosstalk of no more than 40 db
- Time slips corrected on hold times of up to 15 minutes

Voice feature support

- DTMF tones for call signaling
- Call Hold (call placed on hold with HKSW)
- Call Forwarding (on no answer, busy, variable) to local or remote number
- Call Waiting (origination and termination) and Cancel Call Waiting
- Call Return
- Call Trace
- Call Blocking
- Call Screening, Selective Call Pickup, Call Rejection and Anonymous Call Rejection (based on CallerID)
- Call Pickup by dialing a feature code

E-8 Administration Guide

- Speed Dialing by dialing a feature code
- Three Way Calling
- Custom Ringing
- Distinctive Ringing

Glossary

access line: A telephone line reaching from the telephone company central office to a point usually on your premises. Beyond this point the wire is considered inside wiring.

analog: In telecommunications, telephone transmission and/or switching that is not digital. An analog phone transmission is one that was originally intended to carry speech or voice, but may with appropriate modifications be used to carry data of other types.

ANSI (American National Standards Institute): Devises and proposes recommendations for international communications standards. See also *CCITT*.

backbone: A network topology consisting of a single length of cable with multiple network connection points.

bandwidth: The range of frequencies, expressed in Kilobits per second, that can pass over a given data transmission channel within a network. The bandwidth determines the rate at which information can be sent through a channel - the greater the bandwidth, the more information that can be sent in a given amount of time.

baud rate: The rate of the signaling speed of a transmission medium.

bit: A binary digit; the smallest unit of data in the binary counting system. A bit has a value of either 0 or 1.

bits per second (bps): A measure of the actual data transmission rate. The bps rate may be equal to or greater than the baud rate, depending on the modulation technique used to encode bits into each baud interval. The correct term to use when describing modem data transfer speeds.

bps: See *bits per second*.

branch: A length of cable in a star network that goes from the center of the star to a wall jack.

broadcast: A network transaction that sends data to all hosts connected to the network.

burstiness: Data that uses bandwidth only sporadically; that is, information that does not use the total bandwidth of a circuit 100 percent of the time. During pauses, channels are idle, and no traffic flows across them in either direction. Interactive and LAN-to-LAN data is bursty in nature, because it is sent intermittently, and between data transmissions the channel experiences idle time waiting for the DTEs to respond to transmitted data user's input and waiting for the user to send more data.

byte: A group of bits, normally eight, which represent one data character.

CallerID: A feature that allows the called customer premises equipment (CPE) to receive a calling party's directory number during the call establishment phase.

CCITT (Comite Consultatif International Telegraphique et Telephonique): International Consultative Committee for Telegraphy and Telephony, a standards organization that devises and proposes recommendations for international communications. See also *ANSI (American National Standards Institute)*.

CHAP (Challenge Handshake Protocol): A method for ensuring secure network access and communications.

Class A, B, and C networks: The values assigned to the first few bits in an IP network address determine which class designation the network has. In decimal notation, Class A network addresses range from 1.X.X.X to 126.X.X.X, Class B network addresses range from 128.1.X.X to 191.254.X.X, and Class C addresses range from 192.0.1.X to 223.255.254.X. For more information on IP network address classes, see [Appendix B, "Understanding IP Addressing."](#)

client: An intelligent workstation that makes requests to other computers known as servers. PC computers on a LAN can be clients.

2 Administration Guide

community strings: Sequences of characters that serve much like passwords for devices using SNMP. Different community strings may be used to allow an SNMP user to gather device information or change device configurations.

CRC (Cyclic Redundancy Check): A computational means to ensure the integrity of a block of data. The mathematical function is computed, before the data is transmitted at the originating device. Its numerical value is computed based on the content of the data. This value is compared with a recomputed value of the function at the destination device.

DCE (Data Communications Equipment): Term defined by standards committees that applies to communications equipment, typically modems or printers, as distinct from other devices that attach to the network, typically personal computers or data terminals (DTE). The distinction generally refers to which pins in an RS-232-C connection transmit or receive data. Also see *DTE*.

DHCP (Dynamic Host Configuration Protocol): A service that lets clients on a LAN request configuration information, such as IP host addresses, from a server.

DNS (Domain Name Service): A TCP/IP protocol for discovering and maintaining network resource information distributed among different servers.

download: The process of transferring a file from a server to a client.

DTE (Data Terminal Equipment): Term defined by standards committees, that applies to communications equipment, typically personal computers or data terminals, as distinct from other devices that attach to the network, typically modems or printers (DCE). The distinction generally refers to which pins in an RS-232-C connection transmit or receive data. Pins 2 and 3 are reversed. Also see *DCE*.

EIA (Electronic Industry Association): A North American standards association.

Ethernet: A networking protocol that defines a type of LAN characterized by a 10 Mbps (megabits per second) data rate. Ethernet is used in many mainframe, PC, and UNIX networks, as well as for EtherTalk.

Ethernet address: Sometimes referred to as a hardware address. A 48-bits long number assigned to every Ethernet hardware device. Ethernet addresses are usually expressed as 12-character hexadecimal numbers, where each hexadecimal character (0 through F) represents four binary bits. Do not confuse the Ethernet address of a device with its network address.

firmware: System software stored in a device's memory that controls the device. The Netopia 4753's firmware can be updated.

gateway: A device that connects two or more networks that use different protocols. Gateways provide address translation services, but do not translate data. Gateways must be used in conjunction with special software packages that allow computers to use networking protocols not originally designed for them.

HDLC (High-Level Data Link Control): A generic link-level communications protocol developed by the International Organization for Standardization (ISO). HDLC manages synchronous, code-transparent, serial information transfer over a link connection. See also *SDLC (Synchronous Data Link Control)*.

header: In packets, a header is part of the envelope information that surrounds the actual data being transmitted. In e-mail, a header is usually the address and routing information found at the top of messages.

hop: A single traverse from one node to another on a LAN.

hop count: The number of nodes (routers or other devices) a packet has gone through. If there are six routers between source and destination nodes, the hop count for the packet will be six when it arrives at its destination node. The maximum allowable hop count is usually 15.

host: A single, addressable device on a network. Computers, networked printers, and routers are hosts.

host computer: A communications device that enables users to run applications programs to perform such functions as text editing, program execution, access to data bases, etc.

internet: A set of networks connected together by routers. This is a general term, not to be confused with the large, multi-organizational collection of IP networks known as the Internet. An internet is sometimes also known as an internetwork.

internet address, IP address: Any computing device that uses the Internet Protocol (IP) must be assigned an internet or IP address. This is a 32-bit number assigned by the system administrator, usually written in the form of 4 decimal fields separated by periods, e.g., 192.9.200.1. Part of the internet address is the IP network number (IP network address), and part is the host address (IP host address). All machines on a given IP network use the same IP network number, and each machine has a unique IP host address. The system administrator sets the subnet mask to specify how much of the address is network number and how much is host address. See also *Class A, B, and C networks*.

IP (Internet Protocol): A networking protocol developed for use on computer systems that use the UNIX operating system. Often used with Ethernet cabling systems. In this manual, IP is used as an umbrella term to cover all packets and networking operations that include the use of the Internet Protocol. See also *TCP/IP*.

IP address, IP host address, IP network address: See *internet address*.

IP broadcast: See *broadcast*.

ISP (Internet service provider): A company that provides Internet-related services. Most importantly, an ISP provides Internet access services and products to other companies and consumers.

ITU (International Telecommunication Union): United Nations specialized agency for telecommunications. Successor to CCITT.

LAN (local area network): A privately owned network that offers high-speed communications channels to connect information processing equipment in a limited geographic area.

MIB (management information base): A standardized structure for SNMP management information.

modem: A device used to convert digital signals from a computer into analog signals that can be transmitted across standard analog (not ISDN) telephone lines. Modem is a contraction of modulator-demodulator.

NAT (Network Address Translation): A feature that allows communication between the LAN connected to the Netopia ISDN Router and the Internet using a single IP address, instead of having a separate IP address for each computer on the network.

NetBIOS: A network communications protocol used on PC LANs.

network: A group of computer systems and other computer devices that communicate with one another.

network administrator: A person who coordinates the design, installation, and management of a network. A network administrator is also responsible for troubleshooting and for adding new users to the network.

network log: A record of the names of devices, location of wire pairs, wall-jack numbers, and other information about the network.

node: See *host*.

packet: A group of fixed-length binary digits, including the data and call control signals, that are transmitted through an X.25 packet-switching network as a composite whole. The data, call control signals, and possible error control information are arranged in a predetermined format. Packets do not always travel the same pathway but are arranged in proper sequence at the destination side before forwarding the complete message to an addressee.

4 Administration Guide

packet-switching network: A telecommunications network based on packet-switching technology, wherein a transmission channel is occupied only for the duration of the transmission of the packet.

PAP (PPP authentication protocol): A method for ensuring secure network access.

parameter: A numerical code that controls an aspect of terminal and/or network operation. Parameters control such aspects as page size, data transmission speed, and timing options.

port: A location for passing data in and out of a device, and, in some cases, for attaching other devices or cables.

port number: A number that identifies a TCP/IP-based service. Telnet, for example, is identified with TCP port 23.

POTS (plain old telephone service): Ordinary analog telephone service such as that used for voice transmission, as distinct from digital service.

PPP (Point-to-Point Protocol): A protocol for framing IP packets and transmitting them over a serial line.

protocol: A set of rules for communication, sometimes made up of several smaller sets of rules also called protocols. AppleTalk is a protocol that includes the LocalTalk, EtherTalk, and TokenTalk protocols.

remapping: See *network number remapping*.

RFC (Request for Comment): A series of documents used to exchange information and standards about the Internet.

RIP (Routing Information Protocol): A protocol used for the transmission of IP routing information.

RJ-11: A telephone-industry standard connector type, usually containing four pins.

RJ-45: A telephone-industry standard connector type usually containing eight pins.

router: A device that supports network communications. A router can connect identical network types, such as LocalTalk-to-LocalTalk, or dissimilar network types, such as LocalTalk-to-Ethernet. However—unless a gateway is available—a common protocol, such as TCP/IP, must be used over both networks. Routers may be equipped to provide WAN line support to the LAN devices they serve. They may also provide various management and monitoring functions as well as a variety of configuration capabilities.

routing table: A list of networks maintained by each router on an internet. Information in the routing table helps the router determine the next router to forward packets to.

SDLC (Synchronous Data Link Control): A link-level communications protocol used in an International Business Machines (IBM) Systems Network Architecture (SNA) network that manages synchronous, code-transparent, serial information transfer over a link connection. SDLC is a subset of the more generic HDLC (High-Level Data Link Control) protocol developed by the International Organization for Standardization (ISO).

serial port: A connector on the back of the workstation through which data flows to and from a serial device.

server: A device or system that has been specifically configured to provide a service, usually to a group of clients.

SNMP (Simple Network Management Protocol): A protocol used for communication between management consoles and network devices. The Netopia ISDN Router can be managed through SNMP.

subnet: A network address created by using a subnet mask to specify that a number of bits in an internet address will be used as a subnet number rather than a host address.

subnet mask: A 32-bit number to specify which part of an internet address is the network number, and which part is the host address. When written in binary notation, each bit written as 1 corresponds to 1 bit of network address information. One subnet mask applies to all IP devices on an individual IP network.

TCP/IP (Transmission Control Protocol/Internet Protocol): An open network standard that defines how devices from different manufacturers communicate with each other over one or more interconnected networks. TCP/IP protocols are the foundation of the Internet, a worldwide network of networks connecting businesses, governments, researchers, and educators.

telephone wall cable: 2-pair, 4-pair, or 8-pair, 22- or 24-gauge solid copper wire cable. Telephone wall cable is sometimes called telephone station cable or twisted-pair cable.

TFTP (Trivial File Transfer Protocol): A protocol used to transfer files between IP nodes. TFTP is often used to transfer firmware and configuration information from a UNIX computer acting as a TFTP server to an IP networking device, such as the Netopia ISDN Router.

thicknet: Industry jargon for 10Base5 coaxial cable, the original Ethernet cabling.

thinnet: Industry jargon for 10Base2 coaxial cable, which is thinner (smaller in diameter) than the original Ethernet cabling.

UDP (User Datagram Protocol): A TCP/IP protocol describing how packets reach applications in destination nodes.

wall jack: A small hardware component used to tap into telephone wall cable. An RJ-11 wall jack usually has four pins; an RJ-45 wall jack usually has eight pins.

WAN (wide area network): A network that consists of nodes connected by long-distance transmission media, such as telephone lines. WANs can span a state, a country, or even the world.

WAN IP: In addition to being a router, the Netopia ISDN Router is also an IP address server. There are four protocols it can use to distribute IP addresses over the WAN which include: DHCP, BootP, IPCP, and MacIP. WAN IP is a feature for both the Small Office and Corporate Netopia ISDN Router models.

wiring closet: A central location where a building's telephone and network wiring is connected. Multi-story buildings often have a main wiring closet in the basement and satellite wiring closets on each floor.

Index

Numerics

10Base-T, connecting 5-3

A

add static route 10-8

advanced configuration
 features 9-16

application software 5-2

ATMP 12-12

 tunnel options 12-19

B

back panel 3-4

 ports 3-4

basic firewall 13-17

BootP 10-10

 clients 10-16

broadcasts B-13

C

capabilities 1-2

change static route 10-9

community strings 14-14

configuration

 troubleshooting

 PC A-1

configuration files

 downloading with TFTP 15-8

 downloading with XMODEM 15-11

 uploading with TFTP 15-9

 uploading with XMODEM 15-12

configuration screens

 protecting 13-2

configuring

 with console-based management 6-1, 7-1, 9-1

configuring terminal emulation software 6-2

configuring the console 9-19

connecting to an Ethernet network 5-3

connecting to the configuration screens 9-15

connection profiles

 defined 7-7

console

 configuring 9-19

 connection problems A-2

 screens, connecting to 9-15

console configuration 9-19

console-based management

 configuring with 6-1, 7-1, 9-1

D

D. port 13-9

Data Encryption Standard (DES) 12-12

date and time

 setting 9-17

deciding on an ISP account 2-2

default profile 9-13

default terminal emulation software settings 6-4

delete static route 10-9

DES 12-3, 12-7

designing a new filter set 13-10

DHCP

 defined B-8

DHCP Lease 10-11

DHCP NetBIOS options 10-15

DHCP Relay Agent 10-23

display static routes 10-7

distributing IP addresses B-5

downloading configuration files 15-8, 15-11

 with TFTP 15-8

 with XMODEM 15-11

Dynamic Host Configuration Protocol (DHCP) 10-10

Dynamic Host Configuration Protocol, *see* DHCP

Dynamic WAN 10-10

E

Easy Setup

 connection profile 7-7

- IP setup 7-8
- IPX setup 7-8
- navigating 6-5
- overview 7-1
- quick connection path 7-3
- encryption 12-3, 12-7, 12-12
- Ethernet
 - 5-2
- event history
 - device 14-6
 - WAN 14-5

F

- features 1-2
- filter
 - parts 13-6
 - parts of 13-6
- filter priority 13-5
- filter set
 - adding 13-12
 - display 13-8
- filter sets
 - adding 13-12
 - defined 13-4
 - deleting 13-16
 - disadvantages 13-10
 - modifying 13-16
 - sample (Basic Firewall) 13-16
 - using 13-11
 - viewing 13-15
- filtering example #1 13-9
- filters
 - actions a filter can take 13-6
 - adding to a filter set 13-13
 - defined 13-4
 - deleting 13-15
 - disadvantages of 13-10
 - input 13-13
 - modifying 13-15
 - output 13-13
 - using 13-11
 - viewing 13-15

- firewall 13-16
- firmware files
 - updating with TFTP 15-7
 - updating with XMODEM 15-10
- FTP sessions 13-19
- further reading D-1

G

- general statistics 14-11
- Glossary 1

H

- how to reach us A-4

I

- input filter 3 13-17
- input filters 1 and 2 13-17
- input filters 4 and 5 13-17
- Internet addresses, *see IP addresses*
- Internet Protocol (IP) 10-1
- IP address serving 10-10
- IP addresses B-1
 - about B-1
 - distributing B-5
 - distribution rules B-10
 - static B-8
- IP setup 10-2
- IP trap receivers
 - deleting 14-16
 - modifying 14-16
 - setting 14-16
 - viewing 14-16
- IPsec 12-3, 12-7
- ISP
 - account types 2-2
 - information to obtain 2-3

L

LAN-side filtering 13-27
 LED status 14-3
 LEDs 3-5, 14-3

M

MIBs supported 14-13
 MPPE 12-12
 MS-CHAPv2 12-12
 multiple subnets 10-4

N**NAT**

adding server lists 11-17
 defined 10-1
 Easy Setup Profile 11-6
 IP profile parameters 11-23
 IP setup 11-7
 map lists 11-8
 modifying map lists 11-13
 moving maps 11-15
 outside ranges 11-8
 server lists 11-8

navigating

Easy Setup 6-5

navigating through the configuration screens 9-15

NCSA Telnet 6-3

nested IP subnets B-11

NetBIOS 10-15

NetBIOS scope 10-16

Netopia

connecting to Ethernet, rules 5-3
 connection profile 7-7
 distributing IP addresses 10-10, B-5
 IP setup 7-8
 IPX setup 7-8
 monitoring 14-1
 security 13-1
 system utilities and diagnostics 15-1

Network Address Translation 10-3

see NAT 10-1

network problems A-2

network status overview 14-1

O

output filter 1 13-17

P**packet**

header B-13

password

to protect security screen 13-2

user accounts 13-1

PAT (Port Address Translation) 11-2

permanent virtual circuit 9-3

ping 15-2

ping test, configuring and initiating 15-2

port number

comparisons 13-7

port numbers 13-6

PPTP 12-12

tunnel options 12-3

PVC 9-3

Q

Quick View 14-1

R

RADIUS 13-30

restarting the system 15-12

restricting telnet access 13-3

RIP 10-3

router to serve IP addresses to hosts 10-1

routing tables

IP 10-6, 14-9

S

screens, connecting to 9-15

security

filters 13-4–??

measures to increase 13-1

telnet 13-3

user accounts (passwords) 13-1

- security options screen 13-2
 - protecting 13-2
- Simple Network Management Protocol, *see* *SNMP*
- SNMP
 - community strings 14-14
 - MIBs supported 14-13
 - setup screen 14-14
 - traps 14-15
- src. port 13-9
- static IP addresses B-8
- static route
 - rules of installation 10-9
- static routes 10-3, 10-6
- statistics, WAN 14-11
- strong encryption 12-12
- subnet masks B-3
- subnets B-2–B-5
 - multiple 10-4
 - nested B-11
- subnets and subnet masks B-2
- support
 - technical A-4

T

- TCP/IP stack 5-2
- technical support A-4
- telnet 6-2
 - access 9-15, 13-3
- terminal emulation software
 - configuring 6-2
 - default settings 6-4
- TFTP
 - defined 15-7
 - downloading configuration files 15-8
 - updating firmware 15-7
 - uploading configuration files 15-9
- TFTP, transferring files 15-7
- Trivial File Transfer Protocol (TFTP) 15-7
- Trivial File Transfer Protocol, *see* *TFTP*
- troubleshooting A-1
 - configuration

- PC A-1
- console-based management 7-2
- event histories 14-4
- WAN statistics 14-11
- trusted host 13-18
- trusted subnet 13-18
- tunnel options
 - ATMP 12-19
 - PPTP 12-3
- tunneling 12-2

U

- updating firmware
 - with TFTP 15-7
 - with XMODEM 15-10
- updating Netopia's firmware 15-7
- uploading configuration files 15-9
 - with TFTP 15-9
 - with XMODEM 15-12
- user accounts 13-1
- utilities and diagnostics 15-1

V

- Virtual Private Networks (VPN) 12-1
- voice accounting log 14-8
- voice log 14-7
- VPN 12-1
 - allowing through a firewall 12-21
 - ATMP tunnel options 12-19
 - default answer profile 12-13
 - encryption support 12-12
 - PPTP tunnel options 12-4

W

- WAN
 - event history 14-5
 - statistics 14-11

WAN event history 14-5

Windows NT Domain Name 12-6

X

XMODEM 15-10

XMODEM file transfers

- downloading configuration files 15-11

- updating firmware 15-10

- uploading configuration files 15-12

Limited Warranty and Limitation of Remedies

Netopia warrants to you, the end user, that the Netopia 4753 G.SHDSL Integrated Access Device (the "Product") will be free from defects in materials and workmanship under normal use for a period of one (1) year from date of purchase. Netopia's entire liability and your sole remedy under this warranty during the warranty period is that Netopia shall, at its option, either repair the Product or refund the original purchase price of the Product.

In order to make a claim under this warranty you must comply with the following procedure:

1. Contact Netopia Customer Service within the warranty period to obtain a Return Materials Authorization ("RMA") number.
2. Return the defective Product and proof of purchase, shipping prepaid, to Netopia with the RMA number prominently displayed on the outside of the package.

If you are located outside of the United States or Canada, please contact your dealer in order to arrange for warranty service.

THE ABOVE WARRANTIES ARE MADE BY NETOPIA ALONE, AND THEY ARE THE ONLY WARRANTIES MADE BY ANYONE REGARDING THE ENCLOSED PRODUCT. NETOPIA AND ITS LICENSOR(S) MAKE NO OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, REGARDING THE ENCLOSED PRODUCT. EXCEPT AS OTHERWISE EXPRESSLY PROVIDED ABOVE, NETOPIA AND ITS LICENSOR(S) DO NOT WARRANT, GUARANTEE OR MAKE ANY REPRESENTATION REGARDING THE USE OR THE RESULTS OF THE USE OF THE PRODUCT IN TERMS OF ITS CORRECTNESS, ACCURACY, RELIABILITY, CURRENTNESS, OR OTHERWISE. THE ENTIRE RISK AS TO THE RESULTS AND PERFORMANCE OF THE PRODUCT IS ASSUMED BY YOU. THE EXCLUSION OF IMPLIED WARRANTIES IS NOT PERMITTED BY SOME STATES OR JURISDICTIONS, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU. IN THAT CASE, ANY IMPLIED WARRANTIES ARE LIMITED IN DURATION TO NINETY (90) DAYS FROM THE DATE OF DELIVERY OF THE PRODUCT. THERE MAY BE OTHER RIGHTS THAT YOU MAY HAVE WHICH VARY FROM JURISDICTION TO JURISDICTION.

REGARDLESS OF WHETHER OR NOT ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL NETOPIA, ITS LICENSOR(S) AND THE DIRECTORS, OFFICERS, EMPLOYEES OR AGENTS OF ANY OF THEM BE LIABLE TO YOU FOR ANY CONSEQUENTIAL, INCIDENTAL OR INDIRECT DAMAGES (INCLUDING DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, AND THE LIKE) ARISING OUT THE USE OR INABILITY TO USE THE PRODUCT EVEN IF NETOPIA OR ITS LICENSOR(S) HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATIONS MAY NOT APPLY TO YOU. NETOPIA AND ITS LICENSOR(S) LIABILITY TO YOU FOR ACTUAL DAMAGES FROM ANY CAUSE WHATSOEVER, AND REGARDLESS OF THE FORM OF THE ACTION (WHETHER IN CONTRACT, TORT [INCLUDING NEGLIGENCE], PRODUCT LIABILITY OR OTHERWISE), WILL BE LIMITED TO \$50. v.697

